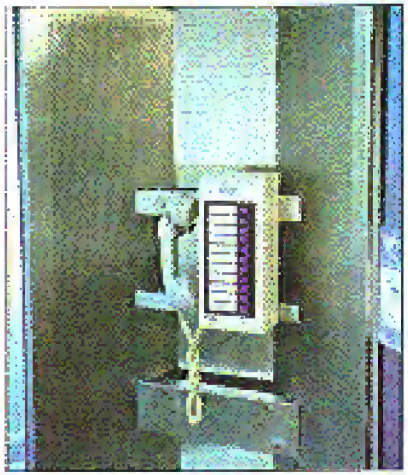
Korean Payphones!



Found on Kunsan Air Base, this phone hooks you to an international operator with one stroke. The buttons all indicate countries to connect to.

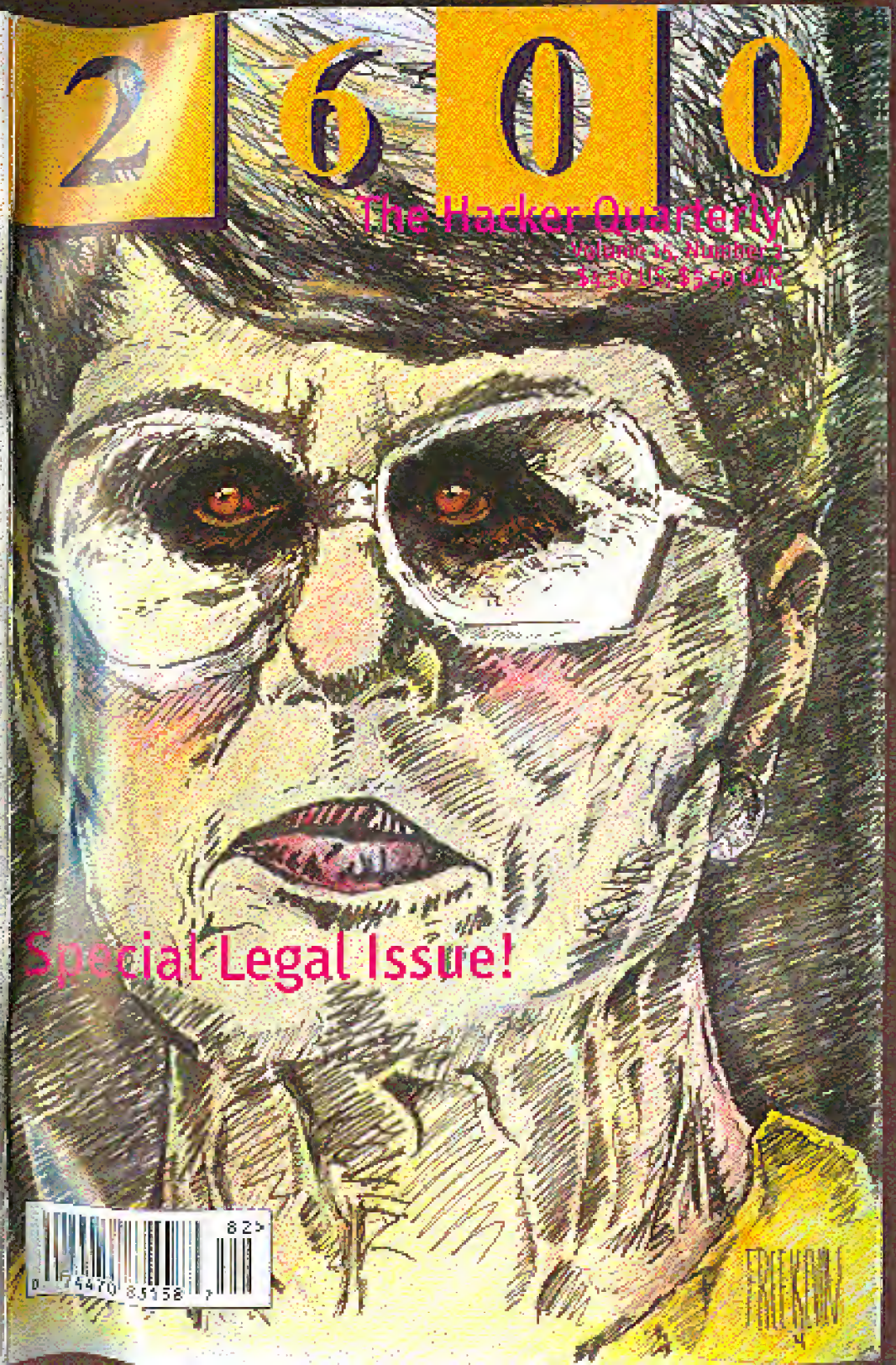
This phone was found on Osan Air Base at the mini mall. It's the typical model for all of the bases.

Blue Boy was found at a Korean barbecue restaurant that is off limits to military personnel.

The phone that might as well be from another planet. Big Red was discovered in a nightclub in Sinlan.

All photos by Jas Ed Carleton

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com



STAFF

"At this moment I do not have a personal relationship with a computer... it got so confusing as to what was on the computer, what wasn't on the computer, what was on the hard drive, what was on the soft drive, that it made it easier for me just to do my work with pen and pencil." - Attorney General Janet Reno, May 24, 1998.


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.8

mQCNAisAvogAAAEEAKDyMmRGmirxG4G3AslxskKpCP71vUP8RzVXpLIa3+Jr10+9
PGFwAPZ3TgJXho5c8c338hstYCowzsl168rROR84J8Rwf+tMz5IBKeKj9LzISW1R
nLNJTm8vBjzHd8mQBeo3794wUMCyEpoqzovu/OUthMLb6UOFC2srX1Hoodr1AAUR
t0Z1bW1hbnV1bE83ZWxsLnNxLnNhLnVz
=W1W3
-----END PGP PUBLIC KEY BLOCK-----
```

s u s t e n a n c e

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.
7 Strong's Lane, Setauket, NY 11733.
Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada - $21 individual, $50 corporate (U.S. Funds).
Overseas - $30 individual, $65 corporate.
Back issues available for 1984-1996 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
2600 Office Line: 516-751-2600, **2600 FAX Line:** 516-474-2677.

LIES

We've gotten pretty used to people getting it wrong. The authorities, the media, the clueless wannabe idiots who never quite get just what it is that hackers are all about. At times the distance they've achieved between themselves and the truth has been humorous. But mostly it's depressing, because when the dust clears, theirs are the perceptions the populace will accept as gospel.

But how far can this go? In recent weeks, a number of us have had to wonder this. Stories and "facts" so bizarre as to be unbelievable even by those people who believe whatever they're told have been surfacing and circulating. And they have brought us to a turning point. Either things are about to get a whole lot worse or maybe, just maybe, people will finally begin to wake up. We'll know soon enough.

It all started with a rather strange article in a magazine called *Signal*. They bill themselves as the "International Armed Forces Communication & Electronics Association's (AFCEA) premiere, award winning magazine for communications and electronics professionals throughout government and industry." In an article entitled "Make-My-Day Server Throws Gauntlet to Network Hackers," *Signal*'s Editor-In-Chief, Clarence A. Robinson, Jr., ramblés on at great length about something called the "Blitzkrieg server," which is able to magically "self-organize and self-heal, recognize an infiltration, isolate it, adapt to it, and create a totally different networking route to overcome an invasion." It also supposedly has all kinds of offensive options just waiting to be used. "These options could eventually end in the destruction of an attacker's network resources." Yeah, right, whatever.

According to the article, the server predicted that "a hacker attack would be targeted at specific U.S. corporations and California state government installations" and that the "attack would be from Japanese nationals with the help of U.S. collaborators affiliated with the 2600 international hacker group."

We found that interesting. Especially since this is the first time that a *machine* has slandered us and our intentions. Since we're relatively sure a human was involved at some stage, we haven't determined who is to blame for this just yet, or even whether the entire story was a piece of fiction created by *Signal* to get attention. That kind of thing doesn't happen very often. However...

Mere days after the *Signal* absurdity, another story appeared in a well respected journal: *The New Republic*. In their "Washington Scene" section was a story entitled "Hack Heaven." It told the tale of Ian Restil, a 15-year-old computer hacker who was terrorizing corporate America.

A first-hand account of Restil's demands for large amounts of money from Jukt Micronics grabs the reader's attention as the story opens. As we read on, we see that the company is tripping over itself to give this brat whatever he wants because, quite frankly, they're terrified of what he can do if he hacks into their databases again. And hackers know this. "Indeed, deals like Ian's are becoming common - so common, in fact, that hacker agents now advertise their commissions on websites. *Computer Insider*, a newsletter for hackers, estimates that about 900 recreational hackers were hired in the last four years by companies they once targeted. Ian's agent, whose business card is emblazoned with the slogan 'super-agent to super-nerds,' claims to represent nearly 300 of them, ages nine to 68."

The article goes on to point out how such deals make it virtually impossible for the police to arrest or prosecute "most hackers" since corporations are so reluctant to come forward and so afraid of what the hackers will do. It's become such a problem that legislation has been brought forward to criminalize such immunity deals between hackers and corporations. But the all-powerful hackers have their own lobbying group - the National Assembly of Hackers - who are vowing to keep the legislation from passing.

We found that impressive. We had no idea that hackers were this powerful. Somehow we had managed to miss this hacker lobbying group, we didn't know this Ian kid at all, and we had never heard of the *Computer Insider* hacker newsletter. But before we could feel the frustration of our ignorance, the world found out something about the article's author, Stephen Glass.

It seems he was a liar. He had made the whole thing up! There was no Ian Restil, no Jukt Micronics, no *Computer Insider*, and no National Assembly of Hackers. And this time, the deceit actually got some attention. The story of the lying journalist was picked up nationwide and reputations were forever tarnished. But in all of the media coverage, we found one thing to be missing. Nobody seemed to care about how the hacker community had been unfairly portrayed. Yes, we know that truth, integrity, and journalism all suffered a black eye because of this pitiful display, but digging a little deeper would have quickly shown how there were human victims as well. The American public *believes* this kind of trash because this view of hackers is constantly reinforced by all of the stories that stop just short of blatant lying. It's not at all uncommon for multinational corporations to be portrayed as helpless victims forever being preyed upon by ruthless hackers. Reality paints a very different picture, as in the case of Kevin Mitnick, a hacker imprisoned for three and a half years with no trial, no bail, and no visitors while his alleged attacks on multinational corporations are questionable at best and, even if proven, trivial and insignificant. Figures given by these corporations on hacker "damages" are believed without question by the authorities while individuals are imprisoned without the opportunity to counter the charges. It may seem incomprehensible that such points are constantly being missed by the media. But, once you do a little digging of your own and see how much of the media these same corporations own, it all becomes painfully clear.

Perhaps you can see now why we find these things so depressing. But all of the above pales in comparison to what we are currently facing.

In early June, it was announced that Dimension Films, in conjunction with Miramax and Miltenium, would be making a film version of *Takedown*.

Why is this important? *Takedown* was the first of the Kevin Mitnick books to be released in 1996, less than a year after his capture in North Carolina. It was also the most flawed, not so much because of the writing, although we could certainly go on at length about the self-centered, egotistical prattling of Tsutomu Shimomura. Rather, it was his and co-writer John Markoff's questionable motives in bringing this story to the American public that have made an increasing number of people take notice. Consider the facts. Markoff had co-written a book called *Cyberpunk* a few years back that had a section devoted to Mitnick, even though he had never interviewed him. Markoff, a reporter for *The New York Times*, managed to somehow get a front page story about Kevin Mitnick published on July 4, 1994. All the story really said was that Mitnick was a fugitive being sought by the FBI. Hardly the kind of thing normally printed on the front page. Even then suspicions were raised. Markoff, in publishing such pieces, was becoming the "Mitnick expert," despite his lack of first-hand knowledge. When Markoff published another front page story in January of 1995 that detailed how the security on Shimomura's computer system had been defeated (again, hardly a front page item), he neglected to mention that the two of them were friends. When Mitnick was captured the following month, Markoff published yet another front page story claiming that he was the prime suspect in the Shimomura incident. Again, an important detail was omitted: Markoff had played an active role in helping Shimomura track down Mitnick in North Carolina. The two had even intercepted telephone traffic between Mitnick and the *2600* offices! And when the book deal was complete less than a week later, Markoff and Shimomura became very wealthy while Mitnick was all but forgotten in prison.

So now there's a movie in the works. Apart from the indignation many of us will feel over the fact that these people will make yet more money off of Mitnick while exploiting a story they practically made up themselves, the real injustice lies in the screenplay itself. While the book was bad and filled with inaccuracies and omissions, the script (written by Howard Rodman), is far worse, a concept admittedly hard to grasp but unfortunately quite true. For in addition to all of the blatant lies of *Takedown*, the film version adds dialogue and situations that are complete fabrications, all in the interests of entertainment.

Only one problem. *Takedown* is supposedly non-fiction. We obtained a copy of the script and can confirm that there is more fantasy in the film version than in the entire *Star Wars* trilogy. And when you consider that this is a film that will be using real people's names and circumstances, the harm it will cause becomes quite apparent.

The anti-Mitnick paranoia is well-established

lies continued..page 54

Where Long Distance Charges Come From

by The Prophet

Most people when calling long distance pay little regard to how charges are calculated. They simply pick up the phone, dial 1+NPA+7, and pay the bill when it arrives. In fact, more than half of AT&T's customers pay so little attention to long distance charges that they pay the AT&T "basic rate," which is the highest price charged by the "Big Three" in America! Literally every AT&T customer would benefit from a savings plan, yet people are lazy and do not make the one phone call that would be required to sign up. So AT&T and others make millions of extra dollars a year as a result.

Most people also do not question why long distance costs money. They simply accept that if they call out of their flat-rate area (if a flat-rate area is even available), the call will cost them a certain amount per minute.

But why is there a per-minute charge for a call between Seattle and Portland, when one can use Internet services between the two cities for free? The answer is a Byzantine system of tolls mandated by the FCC known as "access charges."

Access Charges

The system of "access charges" is at the heart of per-minute charges for voice bandwidth. Every area has an area known as "local toll calling." For instance, the Seattle LATA covers western Washington state with a northern boundary of the Canadian border, the eastern boundary of NPA 509, and the southern boundary of roughly a line from the Columbia River at Longview west to the Pacific coast and east to NPA 509. Calls that are placed between points within the LATA are known as intra-LATA calls, and are routed and priced on a monopoly basis by the LEC (in the Seattle area, predominantly USWest). Calls that cross LATAs, such as a call from Seattle to Portland, are carried by an IXC, such as MCI, which you may choose.

IXCs are where access charges begin. Suppose you place a call from downtown Seattle to downtown Portland. The call is routed from your local switch - anywhere within the LATA - to the access tandem. From there, the call is handed off to your IXC. Your IXC carries the call to the access tandem in Portland, where it hands the call back to USWest along with SS7 routing data. Your friend's phone in Portland rings, and when he answers the circuit is completed. And the billing starts - USWest charges the IXC an "access charge" set by the FCC on both the Seattle and Portland sides. These access charges usually add up to about half of the per-minute charge you pay to the IXC.

If the access charges were to be eliminated, the need to bill by the minute would also be eliminated - there would no longer be an artificial "cost per minute." This would result in the elimination of a great deal of overhead in billing, collections, and customer service. Without access charges, flat-rate long distance would probably be as common as flat-rate local phone service.

LECs Incur Expenses

In general, LECs like access charges. Access charges subsidize the cost of providing residential service in many areas. They also provide a very healthy revenue stream. But they also provide an incentive for people not to spend too long on the phone. With flat rate long distance, people will probably make more phone calls and stay on longer. This is likely to be problematic. Switches are intentionally "under-engineered." Just like ISPs assume every subscriber won't be online at once, phone companies assume that not everyone is going to be using the phone at once. So switches are generally engineered with the "1/7th rule," which holds that on average, only 1/7th (or less) of subscribers will be using the phone at any given time. This works fine when people make short phone calls, but doesn't work nearly as well when a flat-rate unlimited plan is available. The recent explosion in Internet usage has required many LECs to undergo expensive upgrades to local tandems and switches.

In fact, LECs like access charges so much that they think that ISPs should pay them, too. When they began to make expensive upgrades, many LECs petitioned the FCC to force ISPs into the access charge system. ISPs are classified as "enhanced service providers," and are exempt - so far - from per-minute fees, despite the fact that they, like IXCs, carry traffic across LATAs. Pacific Bell was particularly vocal in its criticism of the lack of an access charge revenue stream from ISPs, but became strangely quiet when asked about its explosion in revenue from "second lines," its advertising of "second lines" specifically for Internet use, and in particular its profitable ISP business, pacbell.net.

Thus far, the FCC has ruled against billing ISPs access charges. However, the recent popularity of VOIP has raised interesting concerns. Both the FCC and the telephone industry wonder why a circuit-switched voice call is subject to access charges, but a packet-switched voice call is not. This argument is likely to be resolved soon. The FCC does read all public comments, and posts regular updates on regulatory issues at its website: http://www.fcc.gov.

Bandwidth

One compelling argument in favor of expansion in data services is bandwidth. Domestic bandwidth is at an amazing surplus. In 1992, Sprint's available bandwidth alone could carry every long distance voice call made in the US on a typical business day. It is unlikely that this has changed in the past five years. Sprint has continued to upgrade its existing fiber and lay new fiber. Now, Sprint, MCI, AT&T, LDDS Worldcom/WilTel, Allnet/Frontier, LCI, and numerous other long distance companies have state-of-the-art digital fiber-optic networks, many with similar amounts of bandwidth to Sprint. North America is literally awash in fiber; some fiber is laid and available, but optoelectronics have not yet been installed to put it into use because there aren't any customers for the bandwidth (this fiber is known as "dark fiber"). International bandwidth is more at a premium, but expanding rapidly. Bandwidth is wasted if not used at a given moment in time. Consider then, all of the bandwidth that could be put to good use that is currently unused. The figure is even more staggering when you consider how much bandwidth is wasted in circuit-switched technology. Every voice call occupies a 64k channel, although VOIP users know that good voice quality can be obtained over a 28.8 connection. Circuit switching is inefficient.

Where do we go from here?

According to Department of Commerce statistics, Internet use has grown from three million subscribers in 1994 to over 64 million subscribers today. Clearly the Internet is very popular, and its astounding popularity is likely the result of its low cost and ready accessibility. The FCC is well aware of the Internet's tremendous potential, and has created a 2.4 billion dollar Schools and Libraries fund (http://www.sl-fund.org), to help bring universal Internet access. The status quo is likely to be maintained with respect to the Internet as we now know it. However, the future of enhanced services, such as VOIP and videoconferencing, is very much in doubt. If you think that full use of bandwidth is more efficient than access charges, it is important that the FCC know what you think. Through the "enhanced services" provision, they created the Internet - and with the stroke of a pen, at the behest of a telecommunications lobby, they can destroy it. Be sure that your ISP (or you, if you are an ISP) is well informed of access charge issues - what the FCC does is important to you!

Glossary of Terminology

LEC: Local Exchange Carrier, or the local telephone company (USWest, GTE, etc.)

IXC: InterEXchange Carrier, or the long distance company, carries calls between LATAs (Sprint, MCI, etc.)

LATA: Local Access Transport Area

Tandem: Connects the IXC and LEC's networks, also interconnects LEC networks within a LATA

POP: Point of Presence

CO: The LEC's Central Office, connects your telephone to its network. This is where your distance comes from.

Switch: The heart of a CO, switches calls within or between CO's.

ISP: Internet Service Provider (uunet, concentric, netcom, etc.)

VOIP: Voice Over IP (Internet)

Facts About Cable Modems

by jeremy

Is the price of ISDN another word for outrageous? Are modem speeds rapidly losing their luster due to bandwidth-sucking technology? Tired of making your friends guess what your IP is so they can get on your system? Read on - soon your days of frustration may be coming to an end.

Lately you may have noticed cable guys frantically working on your cable lines outside of your home or apartment. What you may not know is they're actually preparing for you to move into the next step of high-speed, low-cost Internet connectivity. Some of you may already be using 500K cable access as your means of connection, but most of you have only heard rumors or have gotten promises from your cable company about the high-speed connection. Don't lose hope yet. Cable companies around the world are uniting with your local ISPs to bring this connection to your home or business at an affordable cost.

How does this work? The concept is very simple. Your cable company uses a special transceiver which takes a dedicated feed, a very high speed connection, anywhere from 1meg's on up, and broadcasts this bandwidth over RF transmissions via television cable to smaller transceivers located in your home or office. The cable providers dedicate a channel, or frequency, to the transmit and receive of the cable modem. Each modem in the field is then configured to utilize these transmission frequencies which allows them to connect to your cable provider. Here's the catch, and also the reason why it's probably not available in your area. In order for you to transmit and receive at 500K, your cable lines have to be replaced with fiber optic cable, as well as amplifiers which allow two-way communication. Right now most cable only flows in one direction - you never needed anything else. But now in order to take us into this next step in Internet connectivity, all those lines and amplifiers and other related cable equipment need to be replaced. The major problem with this is the availability of this new equipment. The demand for it has overwhelmed cable equipment manufacturers to the point where they have to limit the amount of equipment cable companies can order. One cable company revealed to me that they are only authorized to order a limited supply of equipment, and can only place an order once a year. So basically the cable companies are working as fast as possible to replace equipment, but a lot of it has to do

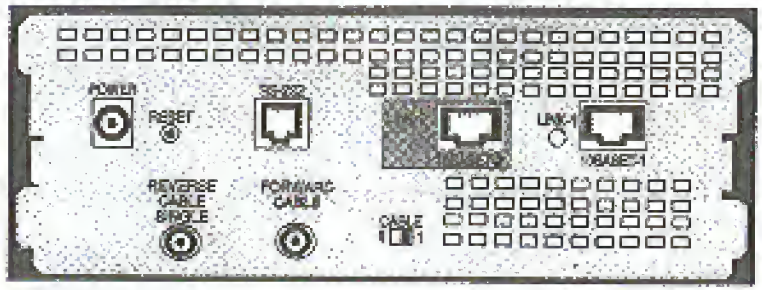


Figure 2: HOMEWorks Universal Rear Panel Connections

with the availability of the equipment. Producing fiber optic cable is not an overnight project.

The client transceiver (the one that goes in your home) is configured via an RS-232 port on the back of the cable modem. This allows you to assign an IP address - each cable modem gets its own IP address for remote management and PROM update from your service provider. This modem setting information is retrieved via setup, subnet, gateway, and a setting to lock out the RS-232 port from further configuration. My service provider does not take advantage of this feature for some reason.

So what are the disadvantages, or rather, what should you expect? The main thing to keep in mind about your cable network is that it is a shared network. Meaning that your total given bandwidth is divided by the amount of users on the system. So, this of course causes problems for you when you have a lot of people on your network who decide to set up their "WaReZ" servers and simply do not care that they are using yours and everyone else's bandwidth so they can trade "GiMeZ." I'll leave it up to you to decide what to do about the bandwidth suckers on your network. You will almost *never* get 500K unless you are the only person on your network, so when your ISP or cable tells you that they have 500K cable modems available, ask them how many people they put on each segment and what total bandwidth is dedicated to the network to get an idea of the actual speeds you can expect. Some ISPs may actually tell you the truth if you ask them what throughput you can consistently expect. I get an average of 350K - 450K on my box, which I consider very good considering the amount of people on my network. 500K is a marketing tool. The cable modems are definitely capable of doing 500K, but first you must have the bandwidth to push it.

Security

You should apply the same security that you would to a machine on a local area network because essentially, that's what the cable network is. The same security holes that are relevant in area LANs are also present in the cable network. If you plan on running a UNIX based OS, then I suggest you run cryptographic software such as ssh (secure shell), and cfs (cryptographic file system) on your server. It is very easy to snoop *any* machine on your cable network unless your provider is using switch technology to segment devices on your cable network. If you're using a MicroSlop based OS, well then there's not much I can do for ya. You will have tons of fun finding all the Microshit 95 people on your cable network who have no clue that they're sharing *all* their services on their machine. I think you should perhaps send a message over their printer giving detailed instructions on how to improve their security, or perhaps you just want to send them a message telling them to eat a bag of shit. It's up to you.

Cost

How much is this? Well, to me this is the best part. Remember, this can vary, and I assume it does quite considerably. For customers in my service area there is a one time $25 setup fee and a monthly $50 dollar charge. It's about $35 for the service and about $10 to lease the cable modem. I'd be very interested in how much people pay for their service in other places around the world. In my opinion, 350K - 450K for $50 a month is a very good price.

Hacking

OK, by now you all may be saying to yourself, what does this have to do with hacking? One of the things that makes the hacking community so strong is its willingness to share information. If we simply keep quiet about the things we know and understand, then our strength and power remains

concealed as well. With this advance in technology, it empowers us to spread the word of technology and the hacker spirit without the suppression from corporate politics and government regulation. You can be in control of your content without worry that Big Brother is going to pull the plug. You now have the ability to tell your side of the story, without the constant media exploitation and distortion that so many of us have long since accepted as a part of the hacker life.

Miscellaneous Notes

I'm using a 500K Zenith cable modem. Zenith also has a one way version, which allows 500K downstream, and modem upstream. They also have a 4meg/s version which I have yet to experience.

Specifications:

RF Modem Transmitter
Maximum Power Output: 150 dBmV 13 dB
Gain Control Range: 20 dB
Frequency Stability: 0.01%
Bandwidth: 1 MHz for -40 dBc (LANHWU-5K)
6 MHz for -40 dBc (LANHWU-4M)
Spurious and Harmonics: 50 dBc
Off-carrier Isolation: 20 dBmV
Frequency Range: 12-108 MHz
Output Impedance: 75 ohms nominal

RF Modem Receiver
Input Range: +10 to -15 dBmV (LANHWU-5K)
+10 to -10 dBmV (LANHWU-4M)
Input Impedance: 75 ohms nominal
50 Kbz LAN HWU-5K
Capture Range: 100 KHz LAN HWU-4M
C/N Performance: 10 -8 for 20 dB C/N (LANHWU-5K)
10 -8 for 24 dB C/N (LANHWU-4M)
Frequency Range: 50-750 MHz

Physical Characteristics
Molded Plastic Cabinet: 15.5" W x 11.75" D x 2.75" H
Weight: 8 lbs.
Connectors: Two Broadband "F" style
One RS-232 (RJ-11)
10BaseT (RJ-45)
(1 or 2 port versions available)

LED Indicators
Power: Power On
Status: Diagnostics and message function
Collision: Packet collisions on broadband
A: Network Activity (RF Carrier)
TX: Transmit data
RX: Receive data
Link 1 (and 2): 10BaseT Link Light(s) (on rear of unit)

Model Numbers
LANHWU-5K 500Kb HomeWorks Universal - single port - 110V
LANHWU2-5K 500Kb HomeWorks Universal - dual port - 110V
LANHWU-5K-I 500Kb HomeWorks Universal - single port - 220V
LANHWU2-5K-I 500Kb HomeWorks Universal - dual port - 220V
LANHWU-4M 4Mb HomeWorks Universal - single port - 110V
LANHWU2-4M 4Mb HomeWorks Universal - dual port - 110V
LANHWU-4M-I 4Mb HomeWorks Universal - single port - 220V
LANHWU2-4M-I 4Mb HomeWorks Universal - dual port - 220V

Zenith Modem information
http://www.zenith.com/main/pc/network_systems/cara.html

FBI PHOENIX DIVISION

SPECIAL AGENT
ANSIR COORDINATOR

201 East Indianola Ave., Suite 400
PHOENIX, AZ 85012

VOICE 602-279-5
FAX 602-650-3
Email:

ANSIR FAX

To:

Pages: 2

Company:

Fax Number:

Although unclassified, this ANSIR FAX computer advisory should be handled as "Sensitive". It is intended for use by corporate security professionals and law enforcement and should not be further disseminated outside of the corporate security and law enforcement environment nor should it be furnished to the media. Unauthorized disclosure of FBI communications could jeopardize ongoing FBI investigations.

The FBI's Awareness of National Security Issues and Response (ANSIR) Program is designed to develop a nationwide communication network among corporate security professionals, law enforcement, and others on a variety of matters. The ANSIR Coordinator in the local FBI field office is the point of contact for all National Security concerns and questions from U.S. corporations.

Future dissemination of ANSIR Program advisories will be provided via ANSIR Email. Recipients of ANSIR FAX should provide their Email addresses to the above listed Email address as soon as possible to continue to receive these notices. ANSIR Email is designed to reach as many as 120,000 recipients to disseminate unclassified threat and warning information in a timely manner.

Message from FBI National Security Division, Washington, D.C.

Attacks on computers running Microsoft Windows NT and Windows 95.

The FBI was advised that on March 2,1998, the U.S. Navy, Department of Energy, National Aeronautics Space Administration and several universities running Microsoft Windows NT and Windows 95 operating systems experienced numerous "denial of service" attacks. The attacks caused computers to crash and crystal what is referred to as the "Blue Screen of Death" accompanied by a "fatal error" message. The "denial of service" attack prevents servers from answering network requirements and can crash individual computers. The specific exploit use in these attacks is known as "Ping Teardrop" or alternatively "Teardrop2." Subtle variations in this exploit (i.e., "Bonk" and "Boink") have also been used in these attacks. The source of these attacks is unknown at this time.

Additional information concerning this matter can be found at the following internet addresses:
www.microsoft.com/security/news-ms2.htm
www.microsoft.com/security/hotfixes.htm
Ciac at www.ciac.org
cert at www.cert.org

Recipients are encouraged to report any information they may have pertaining to this matter to their local FBI field office/ANSIR Coordinator, CIAC representative, or the National Infrastructure Protection Center, FBI Headquarters, (202) 324-8715.

WHAT IS ICA?

by Democritus "Father of Materialism"

Have you ever dialed a number and come across this?

ICAICA**ICA

What Is It?

ICA, or Independent Computing Architecture, is a protocol developed by Citrix Systems, Inc. (http://www.citrix.com) and is used to connect thin clients to phat servers.

Why "PHAT" Servers?

Well, because those servers are exceedingly rich targets. We'll get to that later.

What Is Thin Client Technology?

Well, in case you have been out of the loop for a while, thin client technologies are becoming popular in the corporate environment. The basis for thin client is that thin clients can be simple machines, with very little resources to manage, lowering (in theory) the total cost of ownership (TCO). All applications run on a central server, which centralizes the management of the applications, eases the maintenance of the applications, eases upgrades, all lowering TCO.

The most appealing aspect of thin clients is the fact that those old, tired 486s running DOS can run the Citrix WinFrame Client, connect to the server and run all the latest applications. You don't need to spend $4M to replace 2000 486's with PIIs when you can spend $1M on a few servers loaded with Citrix.

The server, which needs to be pretty hefty, runs all the applications for the clients, and passes only the graphics back to the client. The client software captures the keyboard and mouse and redirects them to the server. The information passing between the client and server are therefore minimal.

Citrix WinFrame allows remote clients to connect by LAN, dial-up, or IP over the Internet. Essentially, it can be used by telecommuters from home, or by road warriors with their laptops. There are clients for DOS, Win 3.1, 95, NT, and Mac which means, regardless of what computer you have, you can connect to the server and do your work, a boon for IT managers.

[The one drawback to Citrix WinFrame is that it is based on Win NT 3.51. Because of this, not all applications will run on it. The version based on Win NT 4.0 was bought out by Microsoft, code named "Hydra." Hydra is in beta testing and will be out later this year.]

Why Are Citrix WinFrame Servers Such Rich Targets?

To begin with, the WinFrame server is a centralized server serving many clients - it therefore needs to be loaded with everything possible the users might need. Even if there are several servers, the domain structure of NT should allow certain users access to everything. Another reason is the defensibility of Citrix. Because Citrix WinFrame can be so heavily fortified against unauthorized access, more can be loaded on it with greater confidence. Since we're looking at Citrix WinFrame servers that have been set up for remote access by users, we're looking at servers that give full access to authorized users to all sorts of databases... of course, we're in here just for curiosity, *not for profit*. That would be highly illegal, and even more unethical. Remember the Hacker's Manifesto.

Um, What Fortifications?

There are several levels of security. The first you've already seen. Without the ICA protocol, you're stuck. This one is simple enough, you can download the client from the web site. Of course, even more basic is the phone number or IP address. These are not going to be published. Also, if you're going to connect over IP, you have to consider firewalls and odd ports.

Unfortunately, the second security level may still stop you here. Citrix WinFrame can be set to provide access only to clients with encryption enabled. Oh, and you can't get the encryption enabled client off the web site - the software is only available from the encryption enabled server. OK, so you use some social engineering and find the client.

The third level is the username and password. Standard NT security and hack stuff here. Note that, if the WinFrame server is connected to a NetWare server, the username and password are synched to the NetWare login and password.

The fourth level is the toughest to hack, and may be unhackable at all (if it exists - this level is a very expensive option, costing roughly $50,000 for 100 users!). The server may be protected by an ACE Server, from Security Dynamics (http://www.security-dynamics.com). The ACE Server is a challenge/response system - when a user logs and is authenticated by the NT/NetWare server, the session is passed to the ACE Server. The Ace Server prompts the user for a PASSCODE. This passcode, anywhere from 4 to 16 alphanumeric characters, is the killer.

The PASSCODE consists of a PIN plus a unique number generated by the SecurID card. (This was mentioned in the Winter issue by Serat.) The SecurID card generates a unique number every 60 seconds - the user has 60 seconds to type in the PIN and the number. If they mistype the number, or the 60 seconds expires, they will have to re-enter the PASSCODE using the newly generated number. The number is unique per 60 seconds, and unique per user!

So How Do I Get In?

If everything is set up as it is supposed to be, you don't. But no system is set up perfectly... and that's why you're a hacker, right?

The hardest part, as I said, is the PASSCODE. NT and NetWare hacks you can find out elsewhere.

The PASSCODE, on the ACE Server, cannot be bypassed from the outside. The SecurID can, however, be removed, disabled, or changed to a password by an administrator with access to the ACE Server console. Ditto with the PIN. Of course, you've got to convince the administrator you're a valid user who's "lost" his SecurID and PIN. But that's not hacking, that's lying. No fun in that.

A Newbie Guide to NT 4.0

by Konceptor
konceptor@hotmail.com

First off, what I have found during my recent adventures into my school's network is extremely useful to the malicious hacker and can lead to serious mishaps should one choose to use it for extreme personal gain. If you choose to use the information you may obtain in a malicious manner, I will frown upon you. You are then not a hacker, but a criminal.

This article describes what I used and how I did it.

What you need: laptop or personal computer with NT 4.0 workstation and an account on the network. A can of AdminAssist (a.k.a. ScanNT). A willingness to explore.

I am currently enrolled in a world-renowned Tech College. My interest in hacking never involved hacking into my own school's network, which is based on NT 4.0. But after a year of attendance (being I am in a laptop class, in which we rent/own our laptops, take them home, dial-up, etc.), I felt a strong urge to test their network security.

"Elite" hackers more than likely know this as a no brainer, but newbies may not be aware of Microlame's stupidity. In my school and on everyone's laptop, we have at least three accounts that the SysAdmins set up for us: our own, the administrators, and guest. If you are in the same scenario as I am, check out your C:\winnt\profiles\ directory and you will se a folder for each of the user accounts for that computer. (Yes, this is kinda the same as Windows 95, except ScanNT won't work.) Each folder is a login for the computer, and also has certain privileges on the network. Note: your account will be there, even if you login as "guest".

More than likely, you too will have an administrator's, or whatever they name it, account, because they like to control and set permissions on the registry and other nonsense. As my C:\winnt\profiles\ is set up:

\administrator
\%myaccount%
\guest.

This means (if you haven't figured it out yet) that you have the option of logging in as administrator on your laptop (before you fall asleep, no student in my school is not the "god" of his laptop).

When you startup an NT 4.0 workstation, you are prompted for your login and password and the domain you are on. I had two domains to start with, REMOTE and my computer's name.

Now, pick up a shareware can of AdminAssist. After you install it on your laptop, it tells you that you are not currently the administrator. Before you can say fuck it, it then asks you if you want administrator rights under your account. Click yes and restart. Presto, you can now crack all the accounts on your laptop and more, which I will get to.

(Note: I was shocked as hell to find out my administrator's password was an easily guessed school phrase, and even more shocked to find out how stupid the administrators are to tell us students that no important information, i.e. grades, records, financing, etc. was kept on the network.)

Before, logged in under my user account, I had access to basic student stuff on my school's network. Under my administrator's account, I now have access to different "other" directories. I almost fell on the floor. In my years of hacking, I have not had even half the hacker's rush as I did on the day I cracked the administrator's account in my own school, and I didn't have to snoop into the server to get it. But the server's log files will record my excursions, so to not give myself away, I just use the library's computers and e-mail the info to a hotmail account, or use a floppy. Logging in under the REMOTE domain narrows unauthorized activity down to 1800 laptops, so if I wanted to not use other computers, I logged in on remote. Except when I used a domain from another computer with their logins and passwords - you get the idea.

My next schedule was to find out how far this account would take me. No, it did not give me total mode. However, I did have access to staff-only related directories and outdated directories, which, when I checked the dates on them, have been there for about a year or two. To make a long story short, I basically copied everything of interest. I checked all outdated files just for shits and grins. I have since obtained .docs of all the IP addresses on the network, copies of .pst's of various teachers and higher-ups who don't password their e-mail access, logins and passwords, grades of everyone in the school, financial records, etc. You name it; I run the school (I will say shame on my school, I didn't know they were corporate. Makes me feel... marketed). I also have access to their .html files, so a little tweak here or there might justify some incorrectness. However, I will not use this information for maliciousness or extreme personal gain.

In my course, I have also had access to various other computers, and have made accounts on my laptop with their logins, passwords, and domains, so as to test their reach on the network.

There are a few computers which I still do not have access to on our network, but that will soon change. Overall, this was an easy access network. Even a newbie should be able to do this one in his sleep. I just proved how easy it is to get everything you want off a network, without having root access to everything. I never had superuser privileges, accounts, or rights. I never had to use finger, port scan, whois, etc. No late night password cracking excursions, no nothing. I just used a few tricks that everyone else can use, but seldom do. The time frame for all this was within a couple of days, except for the e-mail; which... I sure have a lot of e-mails in my Inbox!

Recap of Events

Check out C:\winnt\profiles\. See what accounts are in there; each folder name is a login account.

Download AdminAssist. Install it and crack passwords for accounts on your computer (however, as I recent, I haven't tried L0phtCrack on my network, but plan to.)

With NT 4.0, there are *almost* (I say this because we still have a couple of 95ers on our network) no directories password protected. NT uses authentication of you logging in to your computer. You will have to log in under the account with the most privileges; probably the administrator's. Duh.

Check around the network. Look at all old files. Look at new ones. If you can't access some directories, don't sweat it. You will eventually. Build upon a base. Eventually, even if you are a newbie, you will obtain higher permissions. Just keep at it. Rome wasn't built in a day.

Only make copies. Sysadmins get uptight when they can't find something, or something's been changed. Then they check the logs.

With access to several computers around the school, I was able to incorporate their accounts into my machine, thus providing further exploration, and not having to use each individual computer to do it.

End note: This writ is in no way complete. I encountered various obstructions and highways along the way, and may have left out specific information without knowing it.

Shouts to: ~~darkness~~ and Crunch; let's do some more dumpster diving!

BUILD A MODEM DIVERTER

by digital/Digital
digitaldigital@darkcore.com

A basic modem diverter is simple to make, and requires only a few common components. The design can be expanded in many ways, as well. The concept is not new, and I take no credit for anything other than the design specs given.

Disclaimer

Your work, your actions, your responsibility, your ass.

Function

A modem diverter is a piece of hardware that, when used, diverts an incoming signal on a phone line to another line.

This particular design is for data only. In the most basic setup, it works like this:

If you were to dial a target number (555-4444) from your home location (555-1111), a caller ID or trace would trace back to you at 555-1111. But after going through the diverter, a trace would only trace back to the diverter line 2 at 555-3333!

Here is a sample terminal session:

```
ATZ
OK
ATDT555-2222
CONNECT 2400
```

(At this point, you just have a waiting cursor - the modem on line 2 (outgoing line) is waiting for your commands.)

```
ATZ
OK
ATDT555-4444
CONNECT 2400

Welcome to SomeSystem!

Our Caller ID says you are dialing
in from 555-3333!
```

(Note that the hypothetical trace reads 555-3333, which is line 2 (the outgoing line) of the diverter, and not your location of 555-1111! This is because 555-3333 is the one actually making the call.)

Uses

The applications of such a unit are of obvious value. It can be useful to not have your true location appear on a caller ID or a trace. Note that should the diverter be discovered, the incoming line can be identified and calls made to it cross-referenced with calls from the outgoing line. With enough work, it can still be traced. These issues (and safeguards) will be discussed later.

Another possible use has nothing to do with subterfuge. Suppose you have a BBS or access number in a nearby city that is outside local calling range. If you can place the diverter in a location such that it is a local call to the diverter, and a local call from the diverter to the target, you can make the calls without long distance charges!

Components

Components needed for a basic modem diverter are:

- 2 external modems
- 2 phone lines (1 for incoming, 1 for outgoing)
- 1 null-modem cable (male-male)
- Appropriate phone cables and connectors

The null-modem cable must be of decent quality. Some null-modems (or null-modem adapters) do not connect all the pins. To make sure you have a decent cable, you can either:

- Buy one and try it - if it doesn't work, try another.
- Plug it into a breakout box and make sure the connections are there.
- Don't use the cheapest cable.
- Check the packaging to see if it says whether or not all the pins are connected.

Also, at least one of the modems themselves must be able to be set into DUMB MODE. Some newer modems do not have this ability, others do. There are two typical ways to put a modem into dumb mode: either there is a DIP switch (like the back of USR modems) for SMART MODE/DUMB MODE, or there is a jumper inside the modem to set it to SMART/DUMB. Most older modems have the jumper. The third way - putting the modem into DUMB mode via an AT command - is not desirable and should be avoided. Another term for DUMB mode is "turning off AT command recognition."

Remember that your diverter will only be able to go as fast as the slower of the two modems.

Setup

1. Put one modem into DUMB mode, the other into SMART mode.

2. Configure the DUMB mode modem to auto-answer. A way to do this (not guaranteed to work on all modems) would be ATS0=1&W. Check your modem manual for details. If the modem has a DIP switch to enable auto-answer as well, make sure it is on.

3. Plug the null-modem cable into the butt of both modems.

4. Connect the incoming line to the DUMB mode

modem. This is the modem you will be dialing into when you call the diverter with another modem. Many modems have two RJ-11 jacks on the back (phone jacks). The one you want to plug into is probably labeled WALL, LINE, or TELCO.

5. Connect the outgoing line to the SMART mode modem. Again, the plug you want to plug into is labeled WALL, LINE, or TELCO.

6. Connect power to the modems.

7. Test the diverter by placing a call.

Using The Diverter

To place a call:

Set your terminal software to the baud rate of the slower of your two modems in the diverter. Dial the incoming line of the diverter with your modem. Since we configured it to auto-answer, it will answer your call. But, instead of being connected to a server of some kind, it is connected to the SMART modem. If you are using a terminal program, you would see something like: (comments in ()'s)

```
C:\1AH37337\SIMPLET>simplet.exe
-------------
Welcome to SimpleTERMINAL!
-------------
ATZ
OK
ATDT555-2222
```

(Dial the incoming line of the diverter)

(Ring, ring)

```
CONNECT 2400
```

(You are now connected to the outgoing modem - you can test that you are connected properly by typing AT and hitting ENTER. You should see OK.)

```
AT
OK
```

(Now, you can dial out to your destination)

```
ATDT555-4444
```

(The number you are trying to reach via the diverter.)

(ring, ring)

```
CONNECT 2400
```

At this point, your connection is complete and the diverter should be transparent to the connection in every way. You should be able to type, download, etc. normally.

To End a Call:

A way to force a disconnect on the outgoing modem is to type "+++" (three plus signs in rapid succession) to get back to the command mode of the outgoing (SMART) modem. You can then type ATH and ENTER to force the modem to hang up. You can then disconnect your own modem from the incoming (DUMB) modem to end the call.

You should in theory be able to simply disconnect your own line from the incoming line of the diverter to hang up both sides of the diverter, but I would recommend testing this first before putting it into practice.

Location

It is important for the diverter to be in a secure location. Obviously, you don't want just anyone messing with it - not to mention walking off with it. If you are putting the diverter in the equivalent of "private property" (i.e., somewhere you don't belong) you should get permission where possible and practical. In any case, unless you are going to be near the unit all the time, it is advisable to use a measure of safeguards.

Safeguards and Countermeasures

Normally, this means using simple methods of preventing someone from opening, breaking, or walking off with your diverter. For the more paranoid, this can also include fingerprints, tamper alerts, and so on.

For non-tamper safeguards, put the diverter in a sturdy box or container. You can even remove the modems from their cases and place those in the container to make it look more like a "product." Just be sure to insulate the modem PCBs. The case can be securely shut and/or bolted down. A purloined or counterfeit telco company sticker or logo can also increase the illusion that it's something that is "supposed to be there."

Do not ignore the more low-tech safeguards. If you have a need not to be traced to the diverter or calls, do not call the diverter from your home line or from anywhere else you can be connected to. Do not use components that have your name stenciled into them, or have your home number in the modem's NVRAM. For a truly paranoid safeguard, wipe all fingerprints from the modem, cables, and case, then do all assembly while wearing latex gloves. Perhaps a false trail could be laid by social-engineering someone to hold/handle the box or components before you put it into use - therefore getting *their* fingerprints on it.

For those with electronics knowledge, a tamper-switch could be installed into the box that could trigger some kind of alert once the diverter is opened. This could be triggered to destroy the contents, or send some sort of remote alarm.

Improvements

A measure of security can be added with some work by programming a PIC or microcontroller to sit between the two modems in the diverter and not allow access unless a certain DTMF tone or password is used. This can be combined with the tamper-switch to, for example, change a welcome banner slightly upon someone messing with the diverter. This requires much more work and tools than the basic model, though.

For more information about this design, or any other thoughts or suggestions, email me.

LUCID

by Tom Modern

Project LUCID is a computer network being designed to complement and enhance the international justice system. What it is inevitably used for is anyone's guess. Just like the Internet, it will be (or co-opt) a global system of linked databases. Upon completion, it could include its own hardware, software, OS, programming language, GUI's, etc.

No one really knows for sure, but LUCID is thought by some to stand for "Lucifer Universal Control Identification System". An all seeing, tentacle-like concept used in a tyrannical society in which a person's every move could be collected and stored.

The system would be linked to a Universal Computerized Identification Clearinghouse Resource Center (UCICRC) and could work in conjunction with: personal biometrics cards, ATM/credit/debit cards, clipper chips (now suspected of being installed in phones, televisions, etc.), injectable transponders (implants), etc.

LUCID is being produced by Advanced Technologies Group Inc., and is a copyrighted title. Advanced Technologies has addresses in: West Des Moines, Iowa; Lombard, Illinois; and New Rochelle, NY. The chief designers of LUCID net are Dr. Anthony S. Halaris, M.S. and Jean Paul Creusat, M.D.

Dr. Halaris is an information specialist and president of Advanced Technologies, and is also a professor of computer science at Iona College, NY.

Dr. Creusat is a Medical Officer Investigator for Narcotics Control with the INEOA (International Narcotics Enforcement Officer Association) in the United Nations - NGO (non-government organization) - ECOSOC (Economic and Social Council of the UN). He is also a member of Interpol (international police agency) headquartered in Paris, France and on staff at a company called "Birkmayer Software Development" in New York, NY. Got all that? Good.

Although LUCID's designers claim that it is only a "prospective" system, it is believed that it will be up and running by the year 2000. They also state that they are entrepreneurs and not on any government payroll and that Project LUCID is being developed from private funding.

The term lucid also seems to have a brother in AT&T's Lucent Technologies (formerly Bell Labs). The peculiar Lucent insignia boasts a fiery red circle. A press release presenting its network OS and programming environment called "Inferno," quoted from Dante's classic Inferno - which is about hell.

Peripherals for the Inferno environment contain names such as Styx (hell), Limbo, Merlin, and Spirit.

Other ironies continue with Lucent leasing space at 666 Fifth Ave. in New York City. 666 Fifth Ave. is an ominous looking building with an armor-plated appearance and 666 in blood-red neon high atop the building. It is almost blatant how the suggestive address is plastered on everything. Windows, trash cans, etc.

The 1-800 number for Lucent is 1-800-222-3111. Some prodding on my part yielded the fact that the prefix 222 added equals six. So does the remainder 3111. Six, the number of imperfection, the number of man, and the number of the beast.

AT&T was quoted as stating that it hoped that Lucent Technologies would help "illuminate awareness." All this talk of illumination. Lucifer was the "sun god" in Babylonian times and in the Bible is said to sometimes masquerade as an "angel of light."

Besides Lucent Technologies, something that could work in concert with LUCID net on the information highway could be ISO 9000. ISO 9000 is an industry certification started by the International Organization for Standardization in the 1980's. It specifies a level of quality known as "six-sigma," and is both time consuming and costly to the company involved.

The ISO 9000 spec is said to have been hatched by the Bilderbergers, a group of 125 of the richest, most powerful captains of industry in the world. Although the certification is "voluntary" now, it will probably be mandatory by the year 2000 with setbacks going to the corporations that register late.

Any worldwide computer database that would catalogue, track, and identify the whole populace would need a command center or central brain. Some believe it will be America's NSA (National Security Agency) in Fort Meade, MD. The NSA complex is the second largest building in the world behind the Pentagon, and is nicknamed "The Puzzle Palace." I don't think the United States will be the center of the New World Order though.

A curiosity is a super computer dubbed "The Beast" presented in Dwight L. Kinman's book The World's Last Dictator. In 1973, Larry Gossborn, owner of "Robotics International," received a contract for the production of a computer system in Europe called SWIFT (Society for Worldwide Interbanking Financial Telecommunication). They started building the system in conjunction with the Burroughs Corp. The purpose was to link all financial and authoritarian institutions worldwide.

The mainframe entitled "The Beast" was unveiled with much ceremony in Luxembourg, Belgium in 1977.

BEAST stands for "Brussels Electronic Accounting Surveillance Terminal." It is said to be fully functional and to have already stored an 18-digit code for everyone in the civilized world starting with the numbers "666."

It appears that the hare of the New World Order has begun.

Hacking Lasertag

by Johnk

One of the popular pastimes in this area is to go hang out at the local LaserStorm, play some pool, video games, or even a game of Lasertag. Now the standard LaserStorm franchise allows a little bit of customization to their games of Lasertag and, considering the turnover at a place like LaserStorm, most of the employees have no idea how to customize the game, let alone change it back to the default if someone changed the computer on them. So just in case you're one of those employees and you have legal access to the LaserStorm computer, let's go into a little bit on customizing a game of LaserTag.

System Password

The first thing you need is the system password. You have three options: ask someone who knows, shoulder surf someone who knows, or try the default shipping password of BOB (you would be amazed at how many stores leave this default!).

Player Setup

You don't need the system password for this so if you can't get it, try playing around in here.

Player Unit: Basically the pack number for the player you want to customize.
Name of Player: Self-explanatory.
Player's Alias: Self-explanatory.
Player Team: Green or Red.
Player Shield Number: Level 1 is normal, level 2 allows 2 hits before dead, level 3 allows 3 hits.
Get Last Game Names and Aliases: Self-explanatory
Clear All Players: Self-explanatory
Save This Player's Information: Do this or else you just wasted your time.
Exit: Self-explanatory.

Game Setup

Here is where BOB comes into play. Everything here will modify for all players in game.

Shots In Clip: (1-255) Basically how many shots the player has before he has to re-energize. Change this to 20 and watch the spray and pray players get really annoyed!
Points for Player's Hit: (1-15) Good for changing the chances when playing a team who specializes in padding
Points for Pod Hits: (1-15) Once again change to meet your team's needs. If you don't pod worth a damn, change to 1 point per pod hit
Pod Shot Duration: (1-30 seconds) If you pod, change it to like 15 seconds, if not change to 1 second.
Shield Level: Same as in player setup but for everyone. Good for general confusion.
Length of Games: Tired of paying 10 bucks for a lousy 10 minutes? Change it to 40 minutes! (Warning, people with pacemakers and poor health should consult the local quack before playing a 40 minute game.)
Headset/Shoulder Sensors Display: Turn them off for a good black out game!
Teammate Shooting: Definitely worth the time for disruption. sit back and tag anyone moving and watch your score grow.
Pod Hits Per Player: If you pod, set it to unlimited. Otherwise change it.
Printer: If you want a score printed say yes.

Now you need to click Save, then click Load, and then click Exit to have your new custom game set.

System Setup

Here is where you setup for things like store name, address, and phone number. Be creative – remember, everyone who takes a printed score-sheet with them gets a copy of this information. But of course this is only for store employees to change.

New Password

Hmm, tired of BOB? Enter old password, enter new password, then reenter new password.

Clock

Basic time display functions.
Analog: 12 hour clock.
Digital: 24 hour clock.
Set Font: Change face of digital clock.
Seconds: Display seconds.
Date: Display date.
About the Clock: Help file.

Help Prompt

This only shows you info on the software running and count of games played.

Pod Number Buttons

Lets you reassign pod functions. Usually most arenas do not have enough pods to really change anything in this area.

Conclusion

Well that is it in a nutshell, hope this gives some of you people something to experiment with. The good ones to play with are shields, length, and headsets off. This makes the game much more difficult. If you pod, definitely up the shields to level 3 or least on your own players so you can move to the pod without worry.

One or two other notes: the pack that is carried on the hip has a small AC charger hole on the bottom. This is where they plug the packs in to recharge the battery. This is also where you can reinitialize your pack! Carry with you something that will fit into that hole and when you get shot, plug yourself before you energize. The opposing team will not get a point for your kill. This is why anything resembling plugs are an instant disqualification in tournaments. Plus, if you play lights off you can safely unplug the headset without most being any wiser. Of course you can still be shot in the gun().

Remember, this is for educational purposes only. If you have to use this to win you should probably be sitting in the observation booth. But for fun and diversity, give it a try.

A Note From 3Com

donated by Percival

3Com Security Advisory for CoreBuilder and SuperStack II customers

3Com is issuing a security advisory affecting select CoreBuilder LAN switches and SuperStack II Switch products. This is in response to the widespread distribution of special logins intended for service and recovery procedures issued only by 3Com's Customer Service Organization under conditions of extreme emergency, such as in the event of a customer losing passwords.

Due to this disclosure some 3Com switching products may be vulnerable to security breaches caused by unauthorized access via special logins.

To address these issues, customers should immediately log in to their switches via the following usernames and passwords. They should then proceed to change the password via the appropriate Password parameter to prevent unauthorized access.

CoreBuilder 9000/2500 - username: debug password: synnet
CoreBuilder 3500 (Version 1.0) - username: debug password: synnet
CoreBuilder 7000 - username: tech password: tech
SuperStack II Switch 2200 - username: debug password: synnet
SuperStack II Switch 2700 - username: tech password: tech

The CoreBuilder 3500 (Version 1.1), SuperStack II Switch 3900 and 9300 also have these mechanisms, but the special login password is changed to match the admin level password when the admin level password is changed.

Customers should also immediately change the SNMP Community string from the default to a proprietary and confidential identifier known only to authorized network management staff. This is due to the fact that the admin password is available through a specific proprietary MIB variable when accessed through the read/write SNMP community string.

This issue applies only to the CoreBuilder 2500/6000/3500 and SuperStack II Switch 2200/3900/9300.

Fixed versions of software for CoreBuilder 2500/6000/3500 and SuperStack II Switch 2200/3900/9300 will be available from 3Com by Wednesday 20th May 1998. The CoreBuilder 3500 customers running software version 1.0 may upgrade at no cost to CoreBuilder 3500 Version 1.1 Basic software. This software will be available on the 3Com website by the above date.

General administration of these systems should still be performed through the normal documented usernames and passwords. Other facilities found under these special logins are for diagnostic purposes and should only be used under specific guidance from 3Com's Customer Service Organization.

For more information 3Com has dedicated a hotline at 1-888-225-1793. Outside the United States please contact your local Customer Service Organization location.

USER INSTRUCTIONS FOR THE SENTEX OVATION SYSTEM

Your building has been equipped with a Sentex Ovation system. The following steps are involved in using the visitor entry capability of the Ovation system.

1. The ovation system uses your existing phone lines to let you talk to visitors and allow them access to the building, if you so desire. A visitor is instructed to find your "directory code" and enter your code on the keypad. The system then connects itself to your telephone line and rings your telephone.

2. Upon answering the telephone, you will be in a normal conversation with the visitor. Be sure to speak clearly and strongly so the visitor can hear you over any noise at the door. If you are on the telephone when a visitor attempts to contact you, you will hear 2 tones. This is the call waiting feature. Dialing a "2" on your telephone will place your call on hold and connect you to the visitor. Dialing a "2" again will switch you back to the normal telephone call.

3. Once you have put the normal call on hold and answered the visitor call by pressing a "2", you may take one of two actions: (1) dial a "9" to open the door and let the visitor into the building, (2) dial a "2" to switch back to normal telephone call you have on hold. While connected to the visitor, ten seconds prior to the end of the call, you will begin to hear a short tone each second to signal you the call is about to end. Press the "*" to hang-up without allowing entry.

   If you hang up your phone during a visitor call after putting an outside call on hold, your telephone will ring. When you pick up the phone, you will be connected to the outside call that was put on hold. If you hang up from an outside call while a visitor is waiting, your phone will ring and you will be connected with the visitor when you pick up the phone. Regardless of who is on hold, the system will automatically hang up after three rings.

4. If you dialed a "9", the Ovation system will unlock the door for a preset period of time and a tone will be heard on the speaker.

Just one of many buildings in our area that are adopting this kind of a system, already very common in other parts of the country. Security as strong as touch tones. How intelligent.

Fun With JAVA

by Ray Dios Haque

I run a small chat room that is IRC-based and interfaced though a java client. One day a friend and I were attempting a chat. He was having problems at the time with his TCP/IP protocol. Rather than reinstall his protocol and his Dial Up Networking, he found it rather fun to try surfing anyway. I was on the phone with him when he said, "Hey I can open my mail! (chuckle), just mail the damn thing to me!" Chuckling myself, it suddenly occurred to me that I could indeed mail the chat room to him. We both use Yahoo mail, which as you should know, is a Java enhanced deal. That way you get the look and feel of a real mail program. So why not slide that chat room right in there with the e-mail?

I then viewed the source code for the chat room, and inserted a "codebase" line into the applet. Applets can be run from their current directory in your web page, or from another web page entirely using the "codebase = " line. For example....

```
<applet code="ConferenceRoom.class"
codebase="http://irc.webmaster.com/Java/"
align="baseline" width="500" height="239"
archive="http://irc.webmaster.com/Java/cr.zip"
name="cr">
```

In the example you see that the codebase line has been inserted telling the applet that the class files are stored elsewhere)

Now I mailed him the chat room. Moments later he opened the chat room and found me inside it. But something else even greater happened. The chat room loaded faster than anything we had ever seen before. Why? Because Yahoo's mail server had loaded the room for him! Let me tell you something, Yahoo has some mighty fast mail servers. We're talking T3 action here! This was neat, but it raised other curiosities.

What else would we like to see load faster? I for one enjoy Real Audio and Real Video, but the damn things lag out way to much and I get sick of seeing the "Buffering (X Seconds)" box. Why not drop one of those in an e-mail? Yes it will work, but there is a trick. Typically you see Real Video and Real Audio as a pop up box. Meaning, you click on it, and the "Real" box pops up loading the clip you requested. What you embed Real Audio or Video, you make the source (the page you are on) load the clip for you. The clip will appear as being fastened to the page. So try dropping an embedded clip into an e-mail. You should enjoy the results. This gag also works well with Neshow (which also must be embedded to work). Shortly before writing this article I watched a two hour Roy Rogers movie from www.wasfilms.com, and it never skipped a beat. Even when I went into other windows and surfed, the buffering was damn near non-existent.

The hardest part is finding a page that embeds their Neshow, Real Audio or Real Video, so that you can steal the source code. Here is some sample codes (bullshit free, I have removed the stuff you don't need) that will help you write a nice e-mail for yourself

Real Video/Audio

Of course, you will want to substitute the address I gave you for the one you wish to view. This addy I included for the example is just some shitty Pearl Jam video.

```
<html>
<td>
<embed|src="http://www.calpoly.edu/~rberdes/
mtvblock56.ram" width=176 height=144
controls=IndgeWindow autostart=true
console=cali>
</td>
</html>
```

Troubleshooting

Are you getting back an e-mail which just has the source code you inserted, and not the neat stuff you were hoping for? You may have spaces or page breaks before the <HTML> tag in your e-mail. Delete all spaces. Yahoo is picky about this. Did you enable HTML codes? In Yahoo mail, there is a clickable box that you must check in order for your HTML commands to be used.

Are you getting a blank box (grey) in place of your Real Audio/Video? You may not have entered your source code correctly. Make sure your link really exists, and that you have put in the full address including the "http://".

Getting a security exception error? Some people protect their java and such so that it will only run in certain sources. This is to keep you from running it elsewhere. Very common for porn pages (laugh). A nice way to track the source is to open two windows in your browser. Load the real page inside one window, and then stop the Real Video from loading. Then go to your mail program and restart the clip in there. You will now have the Real Audio/Video running in both windows, at lightning speeds. Enjoy!

AT&T

P.O. Box 105211
Atlanta, Georgia 30384-0211

[redacted]

Account Number: [redacted]

[redacted]:

AT&T has identified a pattern of suspected fraudulent third party calls being billed to your telephone number. Which raises the suspicion that fraud may be occurring. Accordingly, in order to prevent both you and AT&T from potential fraud, AT&T reserves the right to put restrictions as outlined in FCC Tariff No. 1 pg. 43.1, section 2.9.4) has restricted the ability to have AT&T third party calls billed to your number until this matter can be resolved.

If these calls are determined to be fraudulent, every effort will be made to accept to identify the responsible parties. Cases meeting the requirements of eight State and Federal statutes may be referred to law enforcement officials.

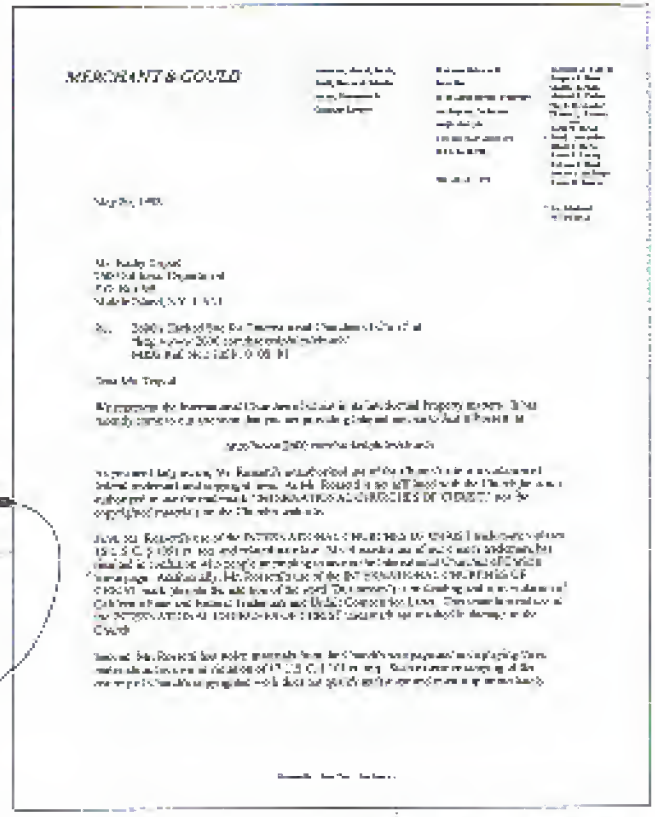
If you wish to discuss this restriction, you may do so in writing to AT&T Corporate Security, P. O. Box 105210, Atlanta, GA 30384-5211 or call 1-800-535-1650 between the hours of 3:30 P.M. and 12:00 A.M. Eastern Time, Monday through Friday.

Sincerely,

[redacted]
SARI ROSENBAUM, Ext. 2048
Security Investigator

This was a fun letter we received a number of months back. The odd thing is that the fraudulent calls never materialized on the bill! Another odd thing is the fact that we already had third number billing blocked. And the final odd thing is the unusual hours these security people are open. We find it a lot more convenient.

Our first veiled threat of a lawsuit in a couple of months and our first ever from a church! It seems these friendly folk are disturbed over the appearance of their hacked web page on our web site. But they had a really strange way of expressing it. We had no idea who this Rossetti guy was until we tracked him down and discovered that he had posted something on their feedback web page that they didn't like. Apparently he told them that he agreed with the



MERCHANT & GOULD

[redacted]

sentiments of whoever had hacked their page and referred to them as a cult, etc. etc. Apparently they took this to mean that he was the culprit and that we were somehow giving him Internet access by displaying the hacked site on our own site. If this twisted reasoning is how they drew religious conclusions, we really feel sorry for them. Regardless, we hope they stop trying to intimidate individuals who were merely expressing an opinion on a page that was asking for just that. As for our copy of the hacked web page—it's news. It's history. And it's staying. Praise The Web.

The Millenium Payphone

by Phluck

Pretty much all Canadian phreaks have become fascinated with the Millenium payphones, and with good reason. These payphones have only been around several years and are a large technical advancement over the previous phones. They are extremely secure against red boxing and pretty much anything else.

In eastern Canada, the advancement was greatly needed. Our previous payphones were very dated (not to mention ugly). In the west, they had newer phones and most of them have not yet been replaced with the new Milleniums. At this point, most of the phones in Manitoba, Ontario, Quebec, and the Maritime Provinces have been upgraded to the Milleniums.

The first thing you will notice about the Millenium phone is the display on it. This displays the time and date, and some advertising usually can be found scrolling underneath that. Below the display there are buttons for volume control, language, and new call. The volume control is self-explanatory. The language button toggles the language in the display between French and English. I'm sure that if another country were to use the phones this wouldn't be there; it's only there because of Canadian language laws. The new call button hangs up and starts a new call, and is pretty useless.

Looking more closely at the phone you will notice that there are two keyholes. There is one on the upper left side of the phone. This one opens up the top part of the phone, allowing the lineman to change settings on it, such as the display message. I have never actually seen a phone with this part open, but it would be really interesting. The other keyhole is on the front of the phone, near the bottom. This one opens up the phone for collecting money.

When you pick up the receiver you hear a dial tone, but don't be fooled, it's actually a recording. There is an annoying voice that speaks over the dial tone telling you how to place your call. Once you drop your quarter in you get a real dial tone, and the mouthpiece and keypad are activated.

One really interesting thing about the Millenium phone is that they don't receive incoming calls. If you try to call the phones, you get a recorded message saying "This phone cannot receive incoming calls." I have heard one interesting story about the operator calling a phreak back who had been harassing her, but I'm not sure if it's true. If it is, it would be really interesting to find out how the phone determines which calls to accept.

According to the official information from Northern Telecom (the makers of the phone), there is a data jack on the it for computers to plug into. On close inspection of the phone I couldn't find this. I assume that this is an optional feature.

The program used for managing these phones is called Millenium Manager. It is built into the phone, and even diagnoses some of its own problems. It has a statistics manager and a logging system. It has an extensive security and alarm system, which calls the telco notifying it when service is needed.

These phones also have really strong fraud protection with lots of fraudulent card and coin detecting devices. There is also something called the "watchdog program" which detects suspicious card use. There isn't too much information on this that I have found, but what I did find was some information on using the system at: http://www.cad-routemaster.com/watchdog.htm

If you want to read more about the phone you can find info at: http://www.nortel.com. It has a list of the phone's features. I'm currently doing research on the technical side of these phones. Once I have enough info I might write another article. Until then, happy phreaking!

How to Hack your ISP

by Krellis

krellis@the-pentagon.com

After seeing the security procedures at my local ISP, both physical and on their servers, I felt I had to inform others of these pathetically lax procedures. If even a few local ISP's are as bad as mine, huge gaping holes exist that must be fixed. I hope to provide enough information here to allow the ISP security services to fix their problems.

Throughout this article, I will refrain from using the real name of my ISP. This is simply because they wouldn't like me much if they saw how I'd tested their security, and I don't want a bunch of malicious little idiots who think they're cool going into my ISP and hacking the shit out of it. I've already spread this information too much, and because of that, the ISP took some new security measures (detailed later) that screwed up any clean, wholesome fun that myself and others could have had.

When I started with this ISP, I had little to no UNIX experience. I now write this as someone who administers his own UNIX system (FreeBSD 2.2.5-RELEASE on a custom kernel). When I started, I couldn't even get my web page set up right. Let me give you an overview of the services provided by my nameless ISP. For US$ 19.95 per month, you get a PPP dialup account, giving access to www, ftp, and all other normal Internet services. You also receive a shell account on their (Linux 2.0.30 based) main server with five MB included storage space. This server serves mail, ftp, www, and telnet for the users of the ISP. Three PPP dial-up access numbers provide access to this server through about five gateways total. The DNS server for this ISP runs on an Intel-based machine at 188 MHz.

Now I will go on to the security holes. One of their biggest mistakes has to be the fact that the /etc/passwd file was (and still is at the time of writing) not shadowed. Any user who has a valid login and password can telnet or ftp in and download this file. A run through a UNIX brute force password file cracker with a 700k or so dictionary file returned some 1500 passwords (not including that of this author). Mind you, this took a long time, even on my Intel Pentium II 266 MHz with 64 megs of RAM. But it worked. As a safety precaution, I have spread a few copies of this password list to secured directories on a number of Internet servers, in case I need to have a copy. No, I won't tell you where it is. Sorry.

Another major error on the part of the security team at my ISP was related to password selection by users. A large number of users had ridiculously easy to guess passwords. I mean, as in "12345" and "abcdefg". At least 100 users (I don't remember the exact number) used their username as their password! Any decent ISP security staff should know not to allow that, and also should disallow the common passwords such as those mentioned above.

One thing I must applaud my ISP for is their sendmail setup. They have configured sendmail not to allow outside, unknown users to send mail through their system. Another system I know of (which has a large user base) allows mail to be sent simply by telneting (anonymously) into the SMTP port and does not IP stamp!

Another problem my ISP has now rectified (due to the circumstances above, I believe) was that they allowed telnet connections from IP addresses outside their network. I (stupidly) told a "friend" the location of the password list, and he promptly accessed a few accounts and wreaked havoc with web pages. This "hacker" (hah! Not really!) screwed up web pages (not saving backups of people's files) and turned them into porno sites, just for personal laughs. Frankly, that *is not funny! Do not do it!* If you come into privileged information, handle it wisely. Don't do what I did, and stupidly give it to people who will be malicious with it. All you are doing when you do that is tipping your hand and ruining it if you ever need to use the information.

Well, that's about it as far as my ISP's security is concerned. There may be more, and I invite anyone else from my area who knows me to send in some more information. I hope this has inspired some ISP security staff to improve the procedures in place on their systems!

HOW TO HACK GAME GURU

by Axon

Shoutouts to the coderz at Studio 3DO who participated in the making of what I believe is one of the best programs written for the die-hard data freaks out there (more specifically, those who love to screw around in hex editors, looking through saved games to try to "transcend" the rules of the game). A retail store I worked at was given a demo copy of Game Guru. My boss told me to just go ahead and keep it, and tell him what exactly it was. He read the box and it looked like something a hacker-type would like. Just reading the package, it seemed almost cheesy. I was unsure how a box with a single floppy and a scant 20-page manual would achieve all of the results that were flaunted in the product description. But indeed I know that coderz can work miracles, so I gave it a shot.

I took it home and installed it on my laptop. I wanted to see what all it would do for Duke Nukem 3D, which was about the only game I had installed on my laptop at the time (before I got an external CD Drive). When I pulled it up, I was asked to "remove the disk, and un-write-protect it." It was strange. I've never seen an install that needed to write to its own disk. Creepy. It installed fine after that. It runs in 4GW protected mode. Rather mundane. When I ran it, I was shocked with a really kick-ass graphic of some virtual game-buddha sort of character. There was even a list of dozens upon dozens of games, and several cheats and codes for them. There were literally dozens for my Duke3D.

As I read though the instruction manual (oh yes, I read the manuals after I install the software - I make a religion of it, but I wished I hadn't practiced that on this occasion), it turned out that this software could only be installed three times. Then the disk would be useless, much like AOL diskettes that are mass-mailed to our doorsteps to prevent us from needing to purchase the media ourselves. Then it struck me. This thing was written by hackers, for hackers. Of course! So I played. I ran a diskcopy of the install disk. Nada. Would not install. It needed "the original Game Guru Install Disk" and wanted me to feed the floppy drive the genuine disk. I ripped up the installed version, and copied it to a 486 I had. After I uncompressed it on the 486 and attempted to run it, it asked me to install it from the install disk, because it wasn't originally installed on that hard drive, but another. I was truly puzzled. Definitely, a work by hackers, for hackers, just like the manual said.

And so I hacked....

What did I find? I decided to go with my diskcopy theory. When a diskcopy is run, it literally lays everything, or so I thought, sector by sector, the same. What in the world was it forgetting to copy? Obviously, the writers of Game Guru knew that something wasn't copied with diskcopy, which I'm sure would be one of the most obvious choices for copying a single disk install. I wanted to know what it wasn't copying. I made three diskcopies of the install, none of which installed (surprise, surprise). I pulled up a copy of PC-Tools by Central Point, which is a must for most hackers who rely on power tools for the PC. It shows all kinds of stuff on the disk, even FAT layout, serial number, and header info. It literally is hex editing the disk instead of individual files on it.

(I found out the serial number, which can be seen with a dos DIR command, is actually reversed. It's in hex. If the serial number shows up in DIR as "5F31-8E4F" it will be in hex on the disk as "4F 8E 31 5F", exactly reversed from the serial number. As you can tell, I tried changing the serial number of the disk to match that of the install disk. No go. (I did learn that trick about the serial number though. I didn't know that until this project.) This is when I used the header viewer. The OEM ID field of the illegitimate floppy read "WIN4.0" or something like that, because the floppy was formatted on a Windows 95 machine, my laptop. Strangely enough, the header view of the true install floppy revealed that the OEM ID was garbled... horribly so. It was a mass of strange characters - the first four characters were not even valid for the OEM-ID field. It typically is restricted to only uppercase letters and numbers, plus a very few symbols.

This really should be done with Central Point's PC tools. Norton just doesn't cut it. The industry standard requires the OEM ID field on the diskette to be in all caps. Norton wouldn't let me enter a letter in lowercase and wouldn't let me insert any higher ascii characters either. Please, for the love of hacking use PC Tools. It rocks. View the OEM ID (Bytes 0003-000A in sector 0 on the disk) of your Game Guru disk (which can be purchased for $9 or so), and jot it down. Then, all you do is diskcopy the install, and edit the fake install's header to make the OEM ID read the same as the original install. Voila! You just hacked Game Guru. Now... you know a ton about copy protection, as this was one of the most challenging schemes I have gone up against. I wanted a copy because floppy disks' shelf lives just suck. There should be no reason I couldn't make a backup. I bought it, and learned a lot while trying to hack it. It is not often that one can hack a program that will help you hack.

You Hacked Game Guru... How Do You Hack With It Now?

When you first run Game Guru, go to the "Edit Settings" menu and activate everything cool. There are quite a few things there to play with. Advanced mode is a must. This opens up options for a very powerful hex editor at your disposal, as well as a few other things. The hex editor has a dual window display. If you load up two files that are the same size in either window, you can compare them. This works well for saved-game files. It will even suggest what possible values the changes represent. If you like to hex out BBS software, like Renegade, you can save the original, and then hex edit a copy of the original, reviewing every difference in the two files at any time. If you open an executable in the hex editor, you can launch an edited version from within Guru, without saving the file itself. If the edit works the way you want, save it. If not, you don't need to worry, just exit the editor.

Anyone who has ever messed around with saved-game files also knows that sometimes the programmers make checksums part of the file. This is a very annoying practice, for when you edit the saved game file, the game will freak out and say that the file is corrupted, so it's erased... with your hard work inside it as well. Game Guru contains a really great CRC Calculator.

Add these great hacking features with the ability to add special Game Guru patches to games (patch codes available all over the net), and the "knowledge base" - a list of cheat codes. The Game Guru File List feature doesn't care about hidden files. They are openly readable, and writeable as well, as long as the other file attributes allow such.

If some of the other many uses for this program are not already beginning to form in your heads, you may not be able to justify buying this program. Otherwise, go get it! Search for it on the web if you can't find it in stores. There is a free version (it looks like Game Guru but doesn't really do much of anything), I think you may be able to get it from Studio 3DO direct, if you can't get it anywhere else.

This has pretty much covered the ins and outs of Game Guru. How to hack it, how to hack with it. It is a good quality program, and I hope that these methods of hacking are not used for piracy, which I do not condone in any way. I do encourage the techniques described here in order to make a backup of the install, because if my drive crashed, I would probably die if I couldn't use it again. Happy Hacking!

LETTERS

Questions

Dear 2600:

Why have I been seeing GTE payphones in Florida? I haven't seen a lot but I have seen a few. Could you help me get the word out about my 2600 meeting? I go but no one ever comes. The meeting is at the Broward mall in Plantation, Florida by the payphones in front of the food court.

Payphone

First off, GTE is a very large local carrier and they have quite a presence in Florida. (People have been known to move to different towns to avoid having to use GTE.) It could also be that you're seeing GTE-manufactured payphones which could be used anywhere. We suggest playing with them to see what their capabilities are and then reporting back to us. As for meetings, we can only help you once you've already established them. Everybody on the planet wants to have meetings in their hometown but it isn't always feasible. If you continued spreading the word and nobody shows up, then it's probably not feasible in your area. But remember, the meetings exist so people can meet other people - even if you're only able to get to one every six months, it's still better to meet twenty new people somewhat infrequently than it is to hang out with the same two or three clods month after month in your local mall.

Dear 2600:

Could you tell me if you have had anyone send you an article on hacking/servicing Meridian phone systems? If not, I got into my Meridian system at work and freaked the cashiers out by renaming the extensions to GOD, SUM, etc., so they'd see "GOD calling" or "calling HIM." I assume know so I don't waste time logging my actions for ya!

reid

We would welcome such an article of mayhem.

Dear 2600:

I recently called an 888 number and it gave me the old line "Your party does not receive blocked calls, blah blah blah). I realize when you call a toll free number your ANI is passed no matter what. However, I wasn't aware that toll free numbers also pass Caller ID information, or was this just some screwy mix up? At the time I called the number, my line was blocked. I have not called the number back using *82. I don't want some guy having my number on his Caller ID box real time. What insight can you give me on this?

Anonymous in Minnesota

Sounds like the number you called went to someone's home or office who had "Anonymous Call Rejection" activated. Caller ID info is passed along on 800/888/877 calls along with ANI. It's the equipment on the terminating end that determines who the called party sees.

Dear 2600:

I am interested in a lifetime subscription and the OTH CDs. However, I would like to maintain some anonymity. Is there any good way to do this? Thanks.

Calime Ishmael

Just use your imagination. You can always take out a PO Box or a maildrop under a fake name. But rest assured that we don't go around sharing our mailing list with anyone, in case that's your concern.

Dear 2600:

Does Janet Reno know what a kernel is?

kris

Does 2600 now?

Dear 2600:

A friend of mine told me that a picture I took might make a good cover for *2600*, and said I should submit it. Do you in fact take submissions for cover photos, and if so, what requirements are there?

Bendzick

Potential cover photos need to be something unique or weird enough to get a double take from most people, yet somehow related to the subject matter of the magazine. Also, we require original photos. Pictures off the net or from digital cameras (anything less than 600 dpi) are not acceptable.

Dear 2600:

This is a notice from my boss here at the Mouse House (Disney). Is this a hoax or what?

"Subject: PHONE SCAM - Beware

"The telephone scam artists are at it again and have recently been calling Disney departments. The caller identifies himself as an AT&T Service Technician who is conducting a test on our telephone lines. He asks that you help complete the test and touch tone (91, zero (0), the pound sign (#) and then hang up. If you comply, you give the requesting individual full access to your telephone line, which allows them to place long distance telephone calls billed to you. The telephone company has advised that this scam has been originating from many of the local jails/prisons. So, please beware."

PbH

We are sick of hearing about this scam - so many people have seen its variations on this letter that it overshadows the scam itself, which is really quite trivial and has been in existence for many years. You simply wind up transferring the caller to an outside line and convincing him to an operator. (Your letter didn't mention hitting the transfer button.) Anyone who falls for something this obvious really deserves a wake-up call. We've had our fill of these "alerts" - it's just not that big a deal.

Dear 2600:

My father just found my copies of *2600* and now he's interested in them. How much would a lifetime subscription cost, including every back issue from 84 to the present?

Asher

Parents can be such pains, can't they? A lifetime sub is still $250 and that gets you 1984 through 1986 back issues plus every issue from now on. All of the other years are $15 each. We're actually embarrassed to add all of that up.

Newsstand Updates

Dear 2600:

I'm a rather new reader of your magazine and I love it. I went to my local Barnes & Noble for the latest issue and searched the stands for a copy, but I couldn't find it anywhere. Then I noticed that there were drawers below some of the stands, and sure enough, I found about 20 copies there. I was rather pissed that they weren't on the shelves, and when I asked a couple of employees, they claimed they'd never even heard of the zine. Well, after a little bit of "hacking," I got them to put the zine out where it normally goes and then put some up by the registers, so hopefully you should get a few more sales from them. Well, I just felt like sharing.

Javelin

Thanks for the support. We depend on our readers to keep an eye out for this sort of thing. Always remember to be polite, though. Otherwise, next time they'll just burn the issues upon arrival.

Dear 2600:

I work at a Barnes & Noble in the Midwest and the *2600* issue that you were talking about on your site did sit in the storeroom for a long time. I know the magazine coordinator, and she didn't say anything to me about any particular reason why they were kept back there. I bought one as soon as they came in, but they sat on the stock shelves for at least a couple of weeks before they were put out on the magazine rack. After they were put on the rack, we of course sold out like we always do.

John Doe

Meetings

Dear 2600:

Two FBI agents were at the meeting in New York. They kept leaning in and listening to the conversations. Just a suggestion, but maybe if it were possible to move

the meeting somewhere else? A suggestion is the World Trade Center. Directly in the middle of the two, three story buildings are a whole load of seats (out in the open) near a waterfall where tourists go. It'll look like we're a bunch of tourists. Good luck.

Twisted circuits

You're missing the entire point of our meetings. We're not trying to hide! That's why we meet in the middle of public areas. Understand? If FBI agents show up (and just how did you know they were FBI agents?), they're welcome in. Anyone dumb enough to do illegal things at a public meeting won't be getting our support anyway. And if the feds wind up doing illegal things, then we're more than happy to provide them with the excess rope which they'll hang themselves.

Dear *2600:*

I noticed that there are meetings in Ann Arbor, MI but I've seen nothing to say when. Is it up to me to find out when or do you know?

Flash

Sorry, that was our mistake in the last issue. All meetings take place on the first Friday of the month, usually between 5 and 8 pm.

Dear *2600:*

I just wanted to write in about something interesting I found out a few months back. I was proudly wearing my 2600 blue box shirt one day, and this man called me over. Apparently, this guy was one of the NYNEX (back when it was still NYNEX) ex-heads of security. He went on a tangent about how my 2600 shirt brought back old memories - about all of the teenagers he used to have arrested for using blue boxes, blah, blah, blah... Then he went on to describe how NYNEX used to send out crews to set up outside the Citicorp center and take pictures of the "kids" attending the meetings. I don't know if what this guy was saying is valid, or even if he did work for NYNEX. If anybody out there works (or worked for) NYNEX (which is now Bell Atlantic), and knows anything of this, please write in.

Dr. Doolittle

Yes, and if any corporations or government agencies have pictures of us, please send them in for our photo gallery. Unless you still plan on suing a man against us or something.

Disturbing News

Dear *2600:*

On March 30, 1998, the computer bulletin board known as *New Times* was censored by Canada's very own RCMP. Why, you ask? Why would a BBS be altered by the Feds? Well, for a reason that might even sound partially justifiable to many of you: because it was distributing information which could instruct people on how to commit crimes. "So what's wrong with that? I don't want those gweddamn headless zunnies running around committing crimes, hackin' computers and rippin' off the phone company!" Well this might sound closely to those of you who watch a lot of television and fear the youth of today. This will sound awful to those of you who fear the government. The police did not actually put an end to any crime in progress, they did not stop any crime before it happened. The police only restricted knowledge, and access to information, a horrible blow to freedom. What will happen in the future?

Yes, on March 30, 1998, an RCMP officer entered my home and instructed me to remove all file bases from *New Times* with the words "hacking" "phreaking" or "carding," in the base title. The file bases were removed on the basis that I am liable for any offenses committed by someone in possession of the information distributed on my BBS. Also removed were the "Pirate Radio" and "Pretty Good Privacy" base. Clearly there are similarities between our government and the famous Orwell novel, *1984*. The RCMP have taken to the role of thought police, effectively regulating what you can and cannot know. When information becomes a liability, you know that Big Brother is watching. Knowledge has become a crime and my BBS has been removed because of information, not because an actual offense has been committed. One file base for an online magazine called *Fuck the World* was removed simply because the officer did not like the title.

When a government targets information for removal, that in itself is a horrible act, but an act of self preservation. When a government outlaws privacy, that shows the very nature of the government's evil. Why, oh why is Pretty Good Privacy on the blacklist? Simple because the controllers cannot read certain people's e-mail. Of course the standard argument that PGP users have something to hide can stop many people from using it. It instills the paranoia that if you use PGP then others will make the assumption that you are a drug dealer or a terrorist. No one will ever assume that you use PGP simply because you do not want others to read your mail. After all, reading another Canadian's mail is legal right? No, it is not. So why is email encryption illegal? Why was Pretty Good Privacy removed from *New Times*?

Canada is a free country, but if you use your free-dom, then it is punishment time, restriction time, regulation time. If you run a hack/phreak BBS then I simply want you to be aware of what happened to *New Times*. If you don't run a BBS but believe in freedom of thought, speech, information, etc., then I want you to be aware of how free we really are. If certain information is outlawed today, then what does the future hold? Literature speaking out against the government? Or even do it-yourself repair books, because people who use them are not spending money? I don't know. I just know that right now knowledge is a crime. Encrypt!

Rainer

New Times Collective

New Times BBS 613-645-1326

Dear *2600:*

While walking through the financial district, I happened across a guy standing in front of a building, reading *2600*. Naturally, I stopped to talk to him, and he explained that his boss (or one of the Mega-Corporations) "caught" him with the magazine. He was advised that it was forbidden to possess it on company property and threatened with disciplinary action. What the hell is this world coming to?

M Davis aka Semi-Spy

Online Idiots

Dear *2600:*

Your magazine explained. It shows that there is a clearly defined line between "hacking" and "using a DoS attack to impress my buddies." However, I guess I'm bowing to the inevitable when I say that I still get disgusted at idiots who insist on being malicious for no reason. If you do this kind of shit, you need to rethink yourself.

Taking aim at average computer users who are ignorant when it comes to things like this is *trash league*. Just because you can get on IRC and type "/whois joe" doesn't give you the right to go slam a lame DOS down the poor guy's/girl's throat, especially since they don't know what's going on, and then flaunt about it. You probably didn't even write the program that did it.

It's not funny. It's stupid. Just because you can send broadcast packets by typing a command in your shell account doesn't make you "elite" or "scary." It does, however, make your "penis smaller" and your "gapped front-teeth wider."

I'm sorry if I seem a tad irate - this was just inspired while I was taking a magical journey in IRC-land (which is becoming more and more the medium of dysfunctional communication) and watching these morons come and harass people who were actually trying to enjoy themselves (however that works on IRC). Just think before you do something next time - is it really worth doing?

Also, your site was recently added to our web proxy server to be blocked, much to my disputing. Unfortunately, there's no way around this as it's done right in the Livingstons that we dial up.

Dave

Wrecker of Universes

Destroyer of Worlds

While what you say is true for the most part, you must also remember that this is only IRC and that IRC is only part of the net, neither of which can be considered "real life." Half the problems we face are caused by people who want to apply "real life" solutions to matters of the net. So don't have a blood vessel over who the little ASCII characters on your screen are doing. Yelling at the TV is far more productive.

Dear *2600:*

Over the past few years, as I have interacted with the hacker community at various occasions I have noticed one thing becoming more and more common: Racism. The hacker community is supposed to be about acceptance and free exchange of information. How can anyone possibly support and believe in this idea when they aren't even capable of grasping the basic facts of reality? There are several races on this earth; however, they are all equal. There are people who say the hacker community will become more accepted once we unite, however, how can this happen when some of us cannot accept other hackers for what they are: people? In short, before the hacker community can escape the generalizations and persecution by the outside world, we must learn to stop those same qualities within our world. Hasn't anyone out there taken "The Conscience of a Hacker," possibly the best piece of hacker literature ever written, seriously?

The Informant

While we take your concerns seriously, it would have been nice if you backed up your claims with some examples and facts. Just saying the entire community is becoming racist is using the same overgeneralization that racism itself thrives on. You must also realize that people often say things online merely to get attention or a reaction. That's not an excuse but at the same time it's not a true indication of who they really are.

Software Concerns

Dear *2600:*

I just found your web site and I was looking to download a copy of QuarkXpressed 0. What the hell is hacking all about anyway? And if you know where I can find Quark, please let me know.

Schrooner

What the hell do you think we're all about? Was there anything on our site to make you think we sell pirated software? Please. Here's a thought. To find out what hacking is all about, explore the site! It does a far better job of explaining it than our words here can do. As for your little quest, maybe the next letter will give you an opportunity.

Dear 2600:

I just found out a way to get any software title for free, and the best thing is, it's free! If you are employed by Babbage's Software you are allowed to "check out" software titles, take them home for a few days, and then bring them back. Then they are re-wrapped and placed back for sale at full price. The company policy at Babbage's (and also Software Etc.) is that this is completely legal since, as their district manager stated "you can't copy CDs anyway." I overheard this while shoulder surfing at my local store and was floored when the manager and three district managers confirmed this. Just a benefit of employment, they said. My question is, do you know if this is legal? Babbage's says yes, but both Microsoft's software piracy and the Business Software Alliance say it is not (I checked). If it is legal, I'll be putting in my application for a part-time job so I can get some of that expensive stuff I want.

Greyhare

This sounds a tad fishy to us. Even if the software stores don't have a conniption over this, we doubt that customers would be pleased to know that the software they buy has already been drooled on by store employees. We're sure the folks at Babbage's will be writing in to clear this one up.

Random Info

Dear 2600:

I am writing in response to the letter in Volume 14, Number 4 which asked about a way to hack the Create-A-Card machines. Their security depends on the fact that the card program is always in the foreground and can't be closed from within. It is possible to get control of the system (usually a PC running Windows 3.1) by having it attempt to print a card when there is no paper. When Windows sees the error it displays an annoying message and sends the Create-A-Card program to the background. While it is in the background, you can tap the program manager icon using the touch screen like a regular mouse. I've only done this once and Windows being what it is crashed before I could do anything really fun. But this flaw provides potential for many great pranks, including possibly reconfiguring the Create-A-Card software. Have fun and remember, "It was like this when I got here."

Luke

Dear 2600:

I just wanted to make a few recommendations that I thought might be of interest to your readers. These are recommended for usefulness and outstanding quantity of information.

ftp://mitpress.mit.edu/telecom-archives. This directory is full of info on various aspects in the telecom arena. A good starting off point for those interested in this field. Personally I only found a few files that weren't worth the taking. Allows 50 anonymous connections and I have generally found it to be unused. The kids must not be doing their research properly.

ftp://ftp.cs.tu-berlin.de/pub/net/phreak/.../ ftp.elf.stuba.sk/pc/ I got this one from a newsgroup and I wish I had clipped the whole message so that I could give credit to whoever posted it. This site is full of all kinds of text files and utilities. I strongly suggest using this mirror due to the fact that ftp.elf.stuba.sk only allows a very few anonymous connections and usually has too many guests. This site is mirrored in several other places but this one tends to be the easiest to access.

Installing Telephones edited by Battle, Charles and Gerald, Luecke. Published by Master Publishing, Inc. This is six bucks at Radio Shack (62-1060) and is a nice text to have around when doing any phone work around the house or office. Very well illustrated, as well. There is no reason not to own this one.

High Noon on the Electronic Frontier - Conceptual Issues in Cyberspace edited by Ludlow, Peter. Published by MIT Press. For information on getting this, try your http://mitpress.mit.edu (mitpress-orders@mit.edu) or your local bookstore. (I feel lucky in the fact that the MIT bookstore is local to me... how sweet it is.) I am sure a good portion of your readers are aware of this one but I feel it cannot be recommended enough. I have found it to be well worth the $30 I paid for it. My only gripe is that it devotes too much time to Mr. Denning. This is a must read for anyone interested in how the net is developing as a society. It provides a fair share of history on some issues that escape coverage in the mass media.

OK, enough of my crap. Have fun.

Atlin

Dear 2600:

I was experimenting with my AT&T model 4615 Cordless Telephone (actually, I was trying to scare the cat) earlier today, when I came across something interesting - a way to listen to radio signals through the phone. The 4615 has two relevant features: 10 channels (so you can find a clear frequency) and an intercom system. The intercom system goes between the base (charger) and handset.

I'm not going to go into the specifics of the intercom, except to say that you have to initiate it via the handset. Also, you can use the blue button on the base (the one you usually use to find the handset if you lose it) to create a tone in the handset ear piece, and if you press "INTCM" on the handset during an intercom session, it will play the same tone through the base.

Anyway, initiate an intercom session (by pressing "INTCM" on the handset). The intercom light on the phone should go on. Then press the blue button on the base and, while the tone is playing, press "INTCM" again on the handset. The intercom light on the handset will go out and you will hear static through the speaker on the base. You can change the channel you are listening to by hitting "CHAN" on the phone.

I've found that you can listen to different conversations and sometimes radio stations using this method. I've also found that different phones will provide different frequencies. (I've tried this on three different phones of the same model.)

SilverStream

Dear 2600:

Here is a little payphone fun you can do to annoy your local stores and or schools. All you do is find out the last four digits of a payphone. If the payphone does not have the number printed and you really want to do this then call someone with Caller ID and find out the number. All you do is dial 790 and the last four digits of the number. Then hang it up and then pick it up and then hang it up again. This little trick here will make the phone ring. This isn't the most efficient trick because I couldn't get it to work in Canada. So for all the Canadians out there, this doesn't apply. This is a common trick, but if you didn't know it then try it.

FiXatioN

First off, many payphones block their number and disable 9x2 so getting the number in that manner frequently won't work. Calling a toll free ANI would be more effective. Second, your 790 trick only works in your local area, which you neglected to tell us. All we know is that you're not in Canada. But the method will work almost anywhere in the States - you simply need to find what exchange is your local ringback.

Dear 2600:

Did you know that if you dial your number and then follow it with the pound (#) button that it accelerates the dialing process and it connects you to the line you are dialing quicker? Isn't that amazing?

Mark Iannucci

About the only thing this is good for in this age of digital switching is making the operator come on a little faster by dialing 0#. Also, it's handy on some overseas calls so the switch knows when you've entered all of the numbers.

Dear 2600:

MediaOne's express service is coming to a town near you. And since they decided to donate a node to my school district, they have started construction on their equipment to receive the fiber link from the nearest hub. They have a board on the wall, in our electrical room, comprised of three Magnavox fiber amplifiers, each with three tie-offs coming off the output, with varying impedance. And the amplifiers are assigned as Internet in (top one, almost always), Internet out, (middle), and residential loop (on the bottom). This content is as raw as it gets - it is direct from the local hub of their network. A way to compromise this little hole has yet to be discovered, although my hands tell me those things get damn hot. Also, after attending a couple of their meetings, in the attempt to sell broadband to whoever has 50 bucks laying around, they are selling the product as "safe, secure, and fast." As many of us know, only one of those is true. And the people they are hiring to do the on-site installs are incredibly dumb. They are button junkies who have little or no computer skill. And don't tell them the modem is for a *nix/Linux box!! They will magically "forget" to stop by your house - from what I have learned, MediaOne is not thrilled about having any other Unix machine on their network. Oh yeah, don't destroy your cable modem, because they have a $600 price tag on them if you destroy or damage them.

Soul Implosion

Dear 2600:

I would like to inform the *2600* readership about more free web space and e-mail services on the net.

www.angelfire.com: free web space.
www.theglobe.com: free web space and e-mail.
www.fortunecity.com: free web space and e-mail
www.tripod.com: free web space

phiberphit

Dear 2600:

I put the "Free Kevin" bumper sticker on my car and had to spend five minutes convincing my mother that Kevin Mitnick wasn't the 15-year-old kid who shot up his high school cafeteria in Oregon. I'm gonna try other means to get the word out, such as passing out flyers with Kevin's story on downtown street corners. I'll keep you posted.

A couple of ANI numbers to have phun with. Pacific Bell - downtown Sacramento: 211-0607 and Roseville (CA) Telephone - Granite Bay: 958?

Desaparecido

Dear 2600:

I'll tell you what little I know about "the bees!" as it was put in that FedEx article.

I used to be a sysadmin for a "large Southeastern bank" who used these SecurID cards for dial-up mainframe access. As explained before, they have clocks synchronized with a dial up server, and a PIN that is derived from that clock with a new one generated every minute. If I remember, it had about nine digits. In addition, the user has a personal PIN that must be used in conjunction with the digits above.

Even if someone did figure out the algorithm or "acquired" it somehow, I really doubt that these things would be crackable. The source code for PGP is freely available, but you don't see that being cracked often. And imagine if your private key changed every minute! The security of these cards is daunting.

However, what I found was that for all the ingenuity and advanced techniques these cards may use, it still remains that these are, after all, typical users. I would wager that in every organization that uses these, 70 percent of the laptop cases have a SecureID card with a sticky note of the Personal PIN stuck to it. I even saw random "checkoutable" laptop cases with the stickynote/SecureID pair in one of the pockets, the absence of which obviously wouldn't have been noticed for some time. So even with these "beasts" the biggest hole (as usual) is with the end user. Inconvenience + typical users = security gap.

Of course, once you get ahold of one of these things you have to know the login screens and syntax (which will be on a handy security admin typed guide with the stickynote/secureID pair). And once you get past those, you have standard host security measures, but the "beast" is now curled up at your feet.

Flint

Dear 2600:

Here's an idea my friend thought of. I call it Caller ID spoofing. OK, we all have three way calling, right? So let's say one person calls another, and this second person places a three way call to another person. Now the first person can talk to the third person. What's so great about that, you ask? Let's say you're supposed to be at work, but instead you ditch and go to a party, and let's assume that you have Caller ID at home. You call your work from the party, ask a friend there to make a three way call to your house. Now you leave a message on your answering machine at home. Your Caller ID says you're calling from home. You have effectively spoofed the source of the call.

skop

OK, now just hold on. Three way calling is hardly a secret and very few people wouldn't immediately suspect its use when faced with a suspicious call. But your real problem here is assuming that there is someone trustworthy at the location you're supposed to be at who will play along with your scheme. And there's always the issue of not being able to be physically located at work while you were supposedly in clear sight making phone calls.

Dear 2600:

890 is my local ANI in Tulsa, Oklahoma. I've heard it works in a big radius of the surrounding area. Possibly the whole state (who cares, it's Oklahoma).

891 does the same for the same area, but only after you enter 7 digits (and it doesn't matter what they are.)

Citrus

Dear 2600:

I love your magazine. You are truly on the subversive edge, fighting on the front lines of the information war. Subscription money coming. I have a couple of things to share with *2600* readers.

For great information on the DoD, there is a free weekly and nonpartisan email newsletter published by the Center For Defense Information. I learn all sorts of fun things reading it every week. The newsletter is called the *Weekly Defense Monitor*. Check it out.

Before I earned the right to call myself a hacker, I worked at a Target store. Target and many other department stores use these little laser gun thingamajigs called "LRT's." This handheld remote gun not only looks cool when you fire it in the dark, it has a more unimaginative purpose. It is used to keep track of store inventory including the location of merchandise in the stock room and on the sales floor. You can also use it to produce lists of what items need to be pulled out of the stock room for the sales floor. It has a condensed but full keyboard, and some combinations of keys let you do some bizarre and rather unexpected things.

The LRT, of course, can be hacked. If the unit gets disabled, it must be reinitialized by the store's host computer. (Sometimes the units break themselves in an hysterical fit of self-destruction.) During the rebooting process, a lot of menus and paths open up for your experimentation pleasure. It is easy to get to a C prompt. From this prompt, you can basically access everything on the store's main computer. I could turn on the fire alarms, kill the lights, open the doors at strange night time hours, visit various archives, and make up false names for gift certificates. Keep in mind that the store rooms all have cameras. I'm sure they saw me hack them, and if I was to steal anything I would have been nailed to the corporate cross.

Also, if you visit Game Works in Seattle, you can access a lot of interesting information just by getting on one of their floor computers. A friend and I were able to (accidentally) crash their Internet cafe by fooling around with the Windows options. I assumed they were lame on security, but when I talked to someone who worked there, I found out how security ignorant the whole staff really was. One guy answered some questions I was almost embarrassed to ask. From the floor computers, you could go in and download some of the games they have. Yes, all of the games projected onto those 40 foot screens run on a DOS shell! Your PC would really be your friend then. Sorry, the network was (as of this summer) closed to outside phone lines.

Mastery

More Fun In Stores

Dear 2600:

A friend of mine bought himself a nice new P200 MMX recently (yes, exactly what I was thinking - that bastard!), but unfortunately he had very little software for it, considering he'd just moved up from a 486-66 for which everything he had was either DOS or WIN3. I was bringing him over a pile of games to play on his machine, and on the way over (I've no idea what possessed me to do this), I walked into Mediascape, a local video game shop. After browsing around for a few minutes, I was on my way out the door when the shoplifting alarm went off! I turned around and tried to explain to the guy behind the corner that it must have been a library book in my bag that set it off (the libraries here put magnetic strips down the spines of all their books!), knowing that if he insisted on searching my bag, there would have been no way I could have convinced him that all the game CD's in there were mine. Luckily he let me go, but I had similar problems at a couple of local bookstores in the days following, and finally found that it was a copy of 2600 stuck in the pages of a notebook at the bottom of my backpack that was causing the problem. It was a copy that I'd picked up at World's Biggest Bookstore (as its name implies, it's a big bookstore here in Toronto, which incidentally is not on your list of stores that carry *2600*, and you've got an entire rack just to yourselves in front of all the other computer mags!), who paste a magnetic sticker inside the front cover of all the *2600* issues! Keep up the good work. I'm looking forward to the next issue.

Corv142

We just manage to cause trouble everywhere we go.

Dear 2600:

Thought you guys might appreciate this: I work in the computer security field and regularly check out your site. I had never picked up your magazine, though, until recently. I was in the Long Branch NJ Barnes and Noble with my two kids. My 10 year old son wanted a gaming zine (to try to break codes). My 4 year old daughter demanded that she get a magazine too. She picked *2600*! I must say I enjoyed it and plan to pick it up regularly. Out of the mouths of babes.

Carole

It's those subliminal messages we slipped into Teletubbies.

2600 Problems

Dear 2600:

I have been a steady reader of *2600* for the past three years and have enjoyed the articles that I have read. I don't actively hack, but I am interested in the ins and outs of how it is done. I was dismayed last fall when I was unable to find a copy of your zine anywhere on its usual hidey holes in the bookstores. I was glad to see the zine back in print in January and just picked up the second issue for this year. I'm glad to see that you stuck it out and were able to start putting out new issues.

Kevin Brown

The thing is, we never stopped printing. Despite the financial nightmares we've been going through, getting the next issue out on time has always been our main priority. Thanks to some very patient people, we were able to do this with virtually no money. By the time you read this, we should be almost entirely out of the woods.

Dear 2600:

I am very disappointed. The hacking/phreaking community promised to be the most intense and influential counterculture faction since the punk rockers of the late 70's and early 80's. Alas, you have sold out, and I blame *2600* - the largest and perhaps most respected icon in the whole hacker world - for much of it.

In numerous editorials you have cited this fact: Hackers aren't criminals. I disagree. Discarding all "wordy" definitions of just what a hacker is and all romanticisms, we find what hacker really means, from the real hackers. Your magazine, hundreds of web pages, programs and text files, as well as the majority of actual documented hacker endeavors, all seem to be about infiltrating or abusing a computer network or another electronic system. Phreaking the phone, remotely hacking Unix systems, and Internet mischief seem to be your specific concerns. Even when programming and other "good" hacker activities are used, they seem to merely facilitate these goals, and are not of any focal interest.

Hacking a system is the equivalent of breaking into someone's house or (in the case of the phone company) office building. If the government allows the production of computers, the right to privately operate one without fear of tampering, destruction, or unreliability should come directly after. It only makes sense. By breaking into a system you are taking up resources and violating privacy. You tiptoe around it - calling this activity "nondestructive hacking." So you break in, but just hang out and have a look around, as opposed to smashing things? Hacking by its very nature is intrusive and forces the individual computer user to seek the aid of computer-manufacturing corporations for education or tools to counter the attack. It is not a liberation or freedom of information. Hacking as you know it is a repeated victimization of the common (uninformed) people. While breaking into a system rarely affects people harmfully, it is the easiest point at which we can deter destruction of or tampering with computer resources remotely. You say people shouldn't go to jail for guessing passwords - and they shouldn't. However, it is indicative of a potential

crime. No one cares that the drunk driver has had alcohol and is behind the wheel for that reason alone - we arrest him because drunk drivers often kill people. That is why hacking, in basically all forms, is a crime. Because, regardless of what you at 2600 do, your readers and everyone associated do not stop at a sensible point. Hackers spread virii, change passwords, cause confusion and frustration in the lives of many total strangers, tarnishing companies' and organizations' reputations, all at their leisure, just for fun.

By distributing your magazine, arguing that hacking isn't a criminal activity, and making your efforts well known to the rest of the world, you have put hackers everywhere under immense pressure. You have turned a once underground activity into a household word, cultivating thousands and teaching them to hack - there were even movies! You have taken something underground, and turned it into "underground" pop culture! In doing so, you sell out so completely that the FBI need only subscribe to enter into your world. You say this is a good thing, the "free flow of information" and all. Well, what are you? The hacker missionaries? The "free flow of information" won't be so cool when the increased hacker populace and computer-crime rate demands legislative attention. When the government passes laws and writes network software making hacking almost impossible, you won't be so glad you taught a generation to hack. They won't be so glad either.

Eric B. AKA Flyable George

Well, gee. You give us credit for an awful lot. Let's look at what you apparently think we should have done. We should have kept quiet so that our little movement would remain "underground." Funny, that's just what the people in those agencies that keep busting in our doors seem to think as well. See, had we only kept quiet, we would have stayed small, and it would have been so much easier to squash us entirely. But now... yeah, we're everywhere. Kinda scary, isn't it? The authorities will one day realize that they're no longer able to manipulate us into extinction. And you have already realized that hacking isn't ever going to be the elitist social club of part-time rebels you want so desperately to be a part of. We're not sure who to feel more sorry for. What we're certain of is that we have nothing to apologize for. We're proud of who we are and where we've gone in the 14 years we've been publishing. We don't support criminal activity but at the same time we don't feel that using a computer system without authorization is remotely similar to breaking into someone's house. But this isn't about us. It's about the many thousands of people out there who are waking up and exploring, learning, and teaching - moving our technology in the direction they want it to go, rather than marching to a pre-determined tune. While we're flattered that you think this is all because of us, we cannot take the credit. But we appreciate your obsession.

Dear 2600:

OK, I know it takes a lot of time and work to put out 2600. I know you have to be able to make money off of what you sell. My question is: Do you think selling advertising space is kinda like selling out? Just some stuff I'd like to know. I think you put together a very informative and educational magazine.

SYCO

We've always felt that advertisements would detract from the main focus of the magazine and raise suspicions (rightfully) that our editorial policy could be affected by advertiser dollars. We'd rather just be accountable to our readers. But we'll open the question up for debate.

Dear 2600:

Please look at my page.

http://www.mbnet.mb.ca/~jkiddell/censored.html

My school division has censored your site - see my page for details. I'm a 16 year old living in Winnipeg, MB (Canada). My entire school division has blocked the 2600 site. It does so through a proxy at dorothy.fgsd.winnipeg.mb.ca. 2600 is only one of many sites which are "Restricted."

Both my parents teach in the school division and I heard rumblings of "the new filter" before today, but I wasn't very worried. After all, I don't usually look at porn during computer science class. Today, the school's Internet connection went down for about 20 minutes, during which time I noticed that Netscape was communicating with a proxy at 206.45.16.37:80. When I noticed our people's connections had started to work, I experienced it firsthand.

Technically, I can open Netscape Prefs and change it from "manual proxy configuration" to "direct Internet connection" which bypasses dorothy but I'm not going to do it to every single computer in the school, especially not every school in the division.

I could understand if it just filtered porn, but 2600? The magazine with no criminal content whatsoever? Isn't this filter just for lazy teachers who don't feel like keeping an eye on their students?

Dave Kiddell

In such cases, the best thing to do is what you did: tell as many people as possible. And to clarify: this isn't really censorship of us as we still exist and are saying what we want to. If we were forced to stop, then that would be censorship of one form or another. What this is is blocking access to you of certain thoughts and ideas by your school.

Dear 2600:

While I don't agree with everything I find in 2600, I still think it is worthwhile reading and would hate to see it go. I know that I would be willing to spend another dollar an issue for awhile until 2600 gets back on its feet. Maybe you should raise the price per issue for a little while then put it back down later when 2600 is more stable. I don't think that most of your readers would object. I know I wouldn't mind.

Curt

We appreciate that but we said at the beginning of this crisis that we didn't want our readers to be paying for our problems. We asked for support in other areas (back issue sales, t-shirts, etc.) and we have received it. That helped us to make it through. When the time comes for a price increase, it will be because of an increase in our expenses - postage, printing, etc. - as has always been the case in the past.

Dear 2600:

I would just like to say that I was going to renew my subscription. You never bothered to send me my last issue, so I'm not going to bother renewing my subscription. Three issues for $22 isn't worth the trouble.

Disappointed

Well, you're a real sorehead. Did you ever stop to think that maybe something happened to your missing issue and that we didn't sit around the office scheming about how we were going to steal your money by skipping our own magazine from you? Things get lost in the mail all the time, co-workers and family members steal your stuff, and, most frequently, people move and their issues don't get forwarded (postal policy). Consider this before you go around hurling accusations. And, had you behaved like a human being and contacted us, we would have replaced your missing issue even if it wasn't our fault. And, for the record, it's $21 for a year.

Comments

Dear 2600:

I'm a new reader of your magazine, and just got the winter issue of 2600. My favorite part would have to be the 1 800 section. I had so much fun with those numbers, and thanks for posting them. On a more personal note, in response to all of you who mailed 2600 saying that hackers suck because we destroy things, and quote me on this, *fuck off*. Thank you and keep up the good work.

Dr. Psycho

That oughta take care of that.

Dear 2600:

Interesting article about the Mobil Speedpass. You stated that it doesn't accept Mac or debit cards. Not true. As stated in any bank's promo regarding these cards, they are accepted anywhere Visa is. Such is true with your debit card. It can be used as a debit card (or if you prefer a few days float), a credit card.

By the way, all my local Barnes & Nobles and Crown books carry your publication. No trouble finding it in the Philadelphia area.

JJ

Pleasantries?

Dear 2600:

You don't know me, I don't know you, but if you are a half decent hacker, you will find who I am soon enough, so enough with the pleasantries. Let me break it down for you. I want to learn to hack. Enough Said. Goodbye.

DramaDame

Dear 2600:

I meant to send this earlier, but kept putting it off. However, after seeing "A Big Misprint" in your latest letters column (Vol. 15, No. 1), I felt I had to respond.

The author of said letter (Sith) complains that the article "How To Be A Real Dick on IRC" is available in many forms and places, and therefore should not have appeared in your zine. Truth be told, I too feel it should not have appeared, but for very different reasons.

Many times you have responded to writers of letters complaining about "Hacker Ethics" (or lack of) by saying that what it is really "all about" is exploration. However, the title of this article immediately jumped out at me as being written from a standpoint of mean-spiritedness. After reading it, that feeling was justified. It basically describes techniques on how to piss people off and how to generally be a dick. This is not an article written about how to explore IRC; this is an article on how to fuck with people, and thus does not fit the ethic (I believe) that you promote.

I found it ironic that in the same issue, there was a letter complaining about this very thing (kicking out the 2600 channel on IRC), and you basically responded by saying that "some hackers get a silly thrill out of this kind of thing" (I'm paraphrasing, of course). How can you condemn something you've just helped promote? Does the right keyboard not see what the left is doing?

I hope that in the future you will take better consideration of the kinds of articles appearing in your zine. I've been a regular reader for some time now, and haven't had much reason to complain until this point. I think most of your readers would rather see articles on IRC security flaws and loopholes than articles describing how to make an asshole of yourself.

Briareos

If we get such articles, we will most likely print them. This one, though offensive to some, provided some valuable insight into how certain people think

letters continued..page 48

FINGERPAINTING AT THE PRECINCT

by The IMC
imc@kingcontent.com

I will never admit to being a smart man, and, if anything, I have spent the greater part of my life being stupid. The most recent occurrence of my stupidity went on display at Yankee Stadium during a rain delay, when I ran across the outfield and did a slip and slide on the tarp that was protecting the infield. No sooner had my momentum died, four rain-coated security guards hauled my dumb ass off into some holding cell while the fans went wild.

I spent some time sobering up in the holding cell until I was told that I would be spending the night in jail. This, by all means, was an unhappy moment, because it meant that I would be hanging out with all of the hoodlums from the South Bronx. Great.

I was moved around from holding cell to holding cell. At one point I found myself in the 44th Precinct standing in front of an Identix machine. Identix is a private company which specializes in biometric computer systems. They make both fingerprint access devices, digital fingerprint systems, and, I suspect, those fingerprint love meters found in arcades and movie theater lobbies. They can be found on the web at http://www.identix.com (it's a poorly designed site.)

The Identix system is basically a Pentium box running OS/2 Warp packaged in a case that has two infrared plates and two VGA monitors. One plate is significantly larger than the other. When a "perp's" fingers are pressed on to the plates, the infrared scans the fingers and displays a realtime image of the scan on the left monitor. The right monitor displays the menu system for the Identix program.

Obviously the menu system is so easy, a cop can operate it. When they drag the perp out of the holding cell, the arresting officer types in the case ID number and other relevent data. Some of my information was already entered and was called up when Officer Dumbass typed in my case ID. He had to enter his name and what I was being charged with.

The menu monitor then instructed the slow-witted law enforcement officer to press down my four fingers on the large pad, then my thumb on the small pad. Then each individual finger was scanned. The process was repeated for both hands. Later, after all fingers were scanned, the program checked to make sure that it could match the individual fingerprints with the aggregate fingerprint of all four fingers. Once verified, the officer can press F8 and send the fingerprints into the NYPD criminal database.

It was my luck that when the officer pressed F8, the machine hung. Officer Dumbass did not know what to do, and was shitting his pants thinking that he had really fucked up the whole NYPD database or something, so he gladly took my advice when I said, "Quick, hit Control-Alt-Delete!" My thinking was that maybe my prints would have been lost, and hopefully ignored.

It took the officer a while to realize that Control was spelled CTRL, and that he was supposed to press the buttons all at once. Upon warmboot, I stared at the screen, in handcuffs, and made some observations:

The Identix machine was running OS/2 Warp.

The machine was on an Ethernet network.

It connected to a couple of file servers without the entering of any passwords.

It repeatedly tried and failed to map some fileserver to the U: drive.

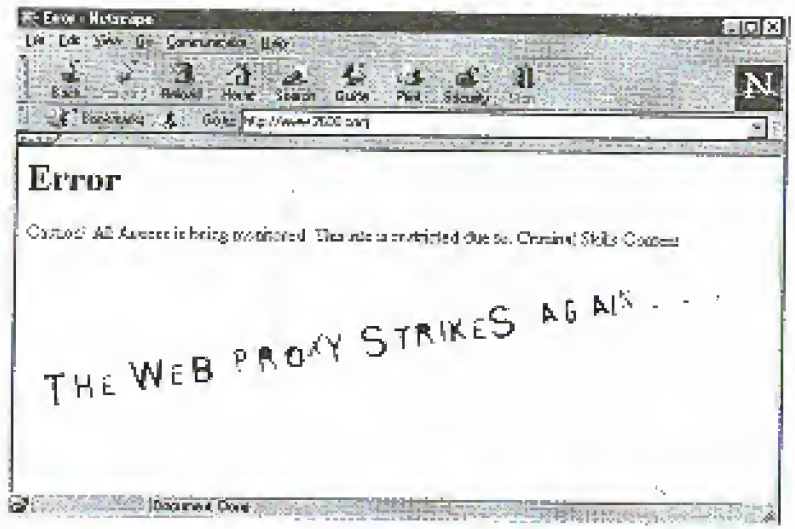
It finally booted up the Identix program, which, in turn, initialized the fingerprint scanners and the second monitor.

The Identix program asked for a name and password, which was obviously precinct specific. Officer Dumbass looked around for awhile and then read the name ("namis") and password ("morpho") out loud as he typed them in.

Later I had to visit another Identix in another precinct because my prints came out too dark. I also had a digital picture taken of me and appended to my record.

The NYPD is still very behind the times and uses far too much paper. This is the reason that it takes needlessly exorbitant amounts of time to process each prisoner. I was arrested for a bullshit charge and it still took them 26 hours to get around to me. I had never been locked up before, and I was going out of my mind.

Which is why I have been thinking about Kevin Mitnick, who hasn't even been tried. Prison sucks and the plight of a prisoner is much worse than what any of us can imagine. I can bet it's even worse for a prisoner who hasn't been given a bail hearing or a trial date after three years.



INTER-TEL PHONE SYSTEMS

by Sundance Beat

Inter-Tel phone systems can be compromised with simple communications programs like ProComm. A little social engineering is needed to get past the receptionist, depending on the voice mail status of the company in question. Every day, Inter-Tel systems are remotely programmed from branch offices. So the company should not expect any foul play during your conversation. What worked for me was as simple as, "Hello. I'm XXXXX calling from Inter-Tel. I have an order to do some programming on your system today. Could you please transfer me to extension 260? Thank you." Sometimes you will get a receptionist with the IQ of lettuce, thereby requiring you to use more patience. You will get, "We don't have an extension 260. Who are you trying to reach?" Simply add, "I'm calling from the company that maintains your telephone system. Extension 260 is the modem extension we use to login to your system." Nine out of ten times you will be transferred.

Logging In: Dialin properties, 300 - 14400, N-8-1

You will need a telephone connected to your modem on the extra RJ port to accomplish a successful login. Boot up ProComm and enter ATD for modem instructions. Just ATD, that's it. Dial the company using the Inter-Tel IMX system, engineer yourself to extension 260. When she says she is going to transfer you and you hear the transfer click, hit enter to execute the manual modem commands and hang up the phone. After you hear the modems chat for a second or two and you hear silence (or have a blank screen), hit enter twice and then you're in. The default database password is just to hit enter. If there is another password, 1437 or 8996 seem to always work. The possibilities of this system are average, unlike the AXXESS system which I will get into later. (You could run a business literally from someone else's AXXESS system without them knowing.) I am working on a more detailed file for this system including specifications and database programming procedures. Sometimes extensions get switched around - valid extensions are 260, 261 (voice mail), 270 (GMX and other systems), 271 (other voice mail systems).

Inter-Tel AXXESS & AXXENT

Now to the mother of digital PBX systems. This is the system that was rated #1 by CTI Magazine. You could run a separate company from this system and no one would even know about it. This system uses proprietary software from Inter-Tel Technologies and there are numerous versions out there. Valid versions in use are: 2.0, 2.1, 2.2, 3.0, 3.1, 4.0, 4.1, 4.2, 4.22, 4.3, and 5.0 is scheduled for release this year. Twenty five percent of systems use 2.0, 25 percent use 3.x, and 35 percent use 4.0-4.22, while the remaining 15 percent use 4.3. I have seen 4.3 via FTP.

The AXXESS also uses extension 260 for remote programming, but also uses 2600 for bigger companies. Barely any social engineering is needed to access these systems mainly because 80 percent of the companies utilizing the AXXESS have IVR or voice automation installed. Voice mail and/or IVR are accessible once inside 260 or 2600.

Logging In: Dialin properties, 9600 - 28800, N-8-1

Execute the AXXESS software and hit F5 to bring up the connection menu. Enter the appropriate information regarding dialing. Say for example the number is 123.456.7890. Dialin properties would be: 11234567890,,,,260 (or 2600). Once the modems chat away and your screen calms down, hit F3 to login. Again, the default password is just hitting enter while 1437 and 8996 also work. Use caution dialing into these systems as the companies probably have T1 with Caller ID activated or standard CO's with Caller ID. The access does support DNIS and ANI - on keysets with LCD's, the caller's name and number can appear if the database is programmed to do so. Companies known to use the AXXESS are Nice Shoes in New York City and Mayer Berkshire, in Wayne, NJ. I will go into database programming techniques further in the future.

If the company does not have IVR or Voice Automation you will need to use the same technique as the IMX systems. Where you would enter ATD, you would just leave the phone number blank in the Dial It properties menu, hit enter, and hang up the phone once the call was transferred.

Beating Access and Account Codes on Inter-Tel Systems

If you are ever in an office that has Inter-Tel installed PBX's and you feel you should add some dollar signs to the phone bill or call your old friend in Peru while in the states, just follow these simple instructions.

Access and Account Codes: Companies that utilize this feature are trying to keep tabs on employees' calling habits. While you would be lucky to guess an employee's four digit account or access code, these few will always work: 8996, 8997, 8998, 8999, and 1437.

Voice Mail Boxes: Voice mail is accessed by either dialing extension 200 or 2000 from an Inter-Tel keyset. When dialed you get IVR or Voice Automation and a superficial menu. Hit * and you are asked to enter your mailbox. Nine times out of 10 the password to a mailbox is the extension number. Example: extension 2342 uses mailbox number 2342 and could have a password of 2342. Yet there will be mailboxes you won't be able to into. This is where the Administrator feature comes in. Usually if there isn't a Telecom Administrator employed at the company, the administrator station is the receptionist's phone. The database of the PBX can also be programmed from this station. To piss off the receptionist, hit the Special or SPCL (sometimes the special button is shaped like an infinity sign or sideways figure 8) and enter a value of 301. This will put the phone into Japanese mode. Anyway, the receptionist's mailbox number is either 100 or 1000, with either no password or 100 or 1000 as the password. When you are into the box, hit 9 to enter into administrator mode. Choose the option for mailbox maintenance, enter the mailbox number you wish to get into, verify it is the correct mailbox, and enter 3 for password change, or just 1 for listen to messages. The beauty is, this can be done from the comfort of your own home by dialing the company's main number.

secure.c

by kasper

Secure monitors your memory and CPU usage on all programs retrieved from ps aux. It writes them to a temporary file (/tmp/.pstab), then parses the data from it and determines whether it is exceeding the limit or not. Set your CPU/MEM limits on lines 75 & 77. I added a dontkill table so if you have some software like rc5 that uses a lot of CPU or MEM and you don't want it killed, just add it to the dontkill table on line 79. You can add as many dontkill's as desired. If the program is not in dontkill and its CPU or MEM exceeds the given limit it will kill -9 the PID. It parses the ps aux table on a one-second interval.

What Good Is Secure?

Secure is useful in protecting yourself from possible loop bugs. Constant loops like the infamous fork() loop would be killed with secure. And if someone on your system is using up your memory the program will be removed by secure. In other words, it just makes your life a little easier.

Testing

Secure was tested on various Linux machines running the slackware distribution on the 2.0.33 kernel, compiled with gcc version 2.7.2.3. The average constant CPU/MEM on our tested machines for secure was CPU: 0.3 MEM: 2.0. The 2.0 memory is primarily because of our fopen() to /tmp/.pstab. If need be, report any questions/comments regarding it to kasper@supernova.digital-galaxy.net.

Known Bugs

Because of the interval every once in a while it may error "unable to load interpreter". If it doesn't load the pstab then it will respawn until it does. In some of our testing the interpreter bug did not occur.

Misc. Information

You might want to add local commands like locate and ls, because if locate or ls displays (prints to standard output) for over a second, which would have the CPU at 99.9, it will be killed.

Warning

I'm not sure, but if tested on other operating systems other than Linux, secure *may* turn on you and *may* do some damage. By compiling this source code you agree that if harm is caused *because of* secure, I *cannot* be held responsible for the damages. Erm.

```
/* keep yourself secure ..

* secure monitors the PIDs on a 1 second basis ...
* secure looks at the CPU and MEM count and if its above its desired
* level it kills the process, I think the code should be cleaned up,
* but for now, oh whell. :B

* -kasper
*/

#include <stdio.h>
#include <stdlib.h>

#define CPULIMIT 90
#define MEMLIMIT 90

char *dontkill[]={"",""};

void parse_pstab(char pstab[]);
void do_pstab();
int checkdontkill(char name[]);
int checksize_for_dontkill();

void main()
{
   if(fork() > 0) exit(0);
   do_pstab();
}

void do_pstab()
{
   char pstab[1024];
   FILE *pst;

our_loop :
   system("s/tmp/.pstab ps aux");
      if(!(pst=fopen("/tmp/.pstab","r"))) main();

         while(!(feof(pst))) {
                  fgets(pstab,sizeof(pstab),pst);
                  parse_pstab(pstab);
   }
   sleep(1);
   fclose(pst);
   goto our_loop;
}

void parse_pstab(char pstab[])
{
   char user[16];
   char pid[8];
   char cpu[8];
   char mem[8];
   char vsz[8];
   char name[16];
         sscanf(pstab,"%s %s %s %s %s %s %s %s %s %s %s",name,pid,cpu,mem
         if(check_dontkill(name))
         kill(atoi(pid),9);
}

int check_dontkill(char name[])
{
   int i=0;

   while(i < checksize_for_dontkill()) {
      if(strcmp(dontkill[i],name)==0) return(0);
         i++;
   }
   return(1);
}

int checksize_for_dontkill()
{
   int i=0;
   while(1) {
   if(dontkill[i]!=NULL) i++;
      else
         return i-1;
   }
}
```

Tips On Generating Fake ID

by DrNick

So you want to get drunk this weekend. Or buy some cigarettes. It is sometimes easier to buy marijuana and take advantage of the black market brought on by the War on Drugs. Or, follow on and learn how to kill your brain cells with alcohol.

Disclaimer

Fake ID is both a state and federal crime. If caught you might not be charged with both, but who knows? Making a fake ID is illegal in many states. It is usually a crime to alter existing state-issued ID, or to create a new fake ID. These crimes include forgery and fraud. They are no fun to get charged with. Using a fake ID to purchase alcohol or cigarettes is often a crime as well. These crimes all differ from state to state, so check your local laws. I do not advocate creating a fake or fraudulent ID. This information is for informational and novelty use only. Do not break any laws. This is not intended for anyone evading prosecution, warrants, etc. I will not hinder prosecution. I do not know how to create a new identity.

Getting ID

You can make it yourself or buy it. Some texts you might read talk about birth certificates and death certificates and all that crap. This article will help you make your own ID. This ID is intended primarily to get you into bars and help you buy beer. Don't even bother trying to fool a cop or fed with it.

Making It Yourself

You will need a combination of the following tools, but these are just guidelines. You should try experimenting with different combinations and seeing which one works best for your IDs! You can probably find all you need here at Staples or your local stationery store.

1. Computer (if you don't have one just forget it)

2. Color scanner for computer (or access to a friend's)

3. Color Printer (hardcore – die-sub printers, for home looking try Epson 400, 600, 800 series)

4. Software (Adobe Photoshop, Paint Shop Pro, etc.)

5. Cutting Tool: Exacto Knife (preferred method) or really sharp short blade or Swiss Army Knife (used to cut out the printed id from the rest of the paper)

6. Adhesive: strong glue stick or double sided scotch tape (experiment here)

7. Posterboard or manila file folder or Metrocard (strengthens the card - experiment here)

8. Contact paper (optional - use only to get the right "look" or "feel")

9. Paper to print front of ID on - high quality inkjet or photoglossy depending on ID. Don't even bother with copy paper.

10. The ID you want to fake (whether it be New York, Connecticut, LILCO, or Bell Atlantic)

11. Nail File (for smoothing ID's edges). Also you might want to try 3M ID cards. They come two to a sheet. Experiment.

How To Make It

1. You need an ID or a template. You need to know what the legitimate 21-year-old version of the ID looks like. It's good if you have a legit ID on hand to compare yours with. Get "The I.D. Checking Guide" (http://www.webbanker.com/pub2.html) as an invaluable reference tool. It is a great book worth ordering. If you need to scan in your own picture or ID make sure it is very clean. Use a high resolution - 720 DPI is good. You must use at least 24 bit resolution. Making your own template is as easy as recognizing the important information on the ID and how to correctly present it.

2. Follow what the template says. Put the picture in the right place. Fill in the right blanks.

3. Find a good medium to print on and work with. Remember, you are going to need a front and back for this ID. I have seen fake NY State IDs using recycled Learner's Permits. The new fake front is glued on top of a learners permit so the back is the same. Sometimes, though, you don't have an old license around. If you don't, then scan the back of the driver's license and print it out on posterboard. Use the posterboard as the back. It's not perfect but close. Again, you are encouraged to experiment and see if you can find something better. This is part of the process and helps you stay on your game as an artist.

4. Print the front out. Use a high quality paper. Photo glossy is not necessary and is sometimes too thick or glossy for the job. Depending on what ID you are imitating you may or may not need a laminating surface.

5. Use a glue stick or double stick tape to adhere the front of your ID to the back.

6. Trim the corners with the knife (if necessary). You might want to use a nail file to smooth the edges on the ID.

Purchasing Fake ID

If you live in a big city (New York), walk down to the business districts (Times Square, 5th Avenue) and you can find some shops. I am not 100% sure as I have never done this myself but my friends have. Look and listen. In New York you can sometimes buy fake ID in the back of luggage shops. Weird but true. It is often some fake looking out-of-state or some bad college ID, but see if it suits your needs. Most of the net is full of crappy novelty ID, nothing to buy beer with. Info on the net will help you make your own.

Using the ID

So, you finally got an ID. One that says you're 21 or 18 or however old you need to be to buy items (to exercise your property rights!). So, now that you've invested $20–$100 you're all set, right? Wrong! Here is free advice. Take it. Kant says the only right acts are those with good intentions. I try. Don't consume alcohol in public where doing so is prohibited by law (i.e., on the street). This is because it is illegal and when some cop finds out you are not only drinking on his streets but not even 21 he will throw a fit. Save yourself the trouble. Whether your ID is successful or not depends on many things. Some are beyond your control, such as a club's policy on fake ID. Some are within your control, such as how you present yourself and what you exude.

Factors beyond your control: The setting: the bar, restaurant, store. Hopefully you can choose a place that is easily passable.

Possibly within your control: your server/bouncer. When in a grocery store *do* go towards the 19-year-old cashier. The younger ones usually care less about this whole ID thing. *Do* take advantage of the Korean/Pakistani immigrant grocer. In the midst of all of Giuliani's "law and order" crackdown, my friend at NYU can still buy his Coronas quite easily. The immigrant clerk questions my friend "Id?" To which my friend replies (with a smile) "Yes ID." Your biggest friend is your great personality. Look happy and confident and you will walk away with the goods. *Don't panic!*

What You Can Do

Know your fake birthday, name, address, zip code and all that info on the card as well as your Zodiac sign.

Go to a place that has accepted your ID in the past! This is my best advice.

When waiting on a line for admission to a club, have the ID ready - be confident!

When you are purchasing at a grocery store or take-out place, it is nice to have it ready to present to the cashier. Try to view it as a formality that you are accustomed to engaging in. You are used to getting carded... remember?

In a restaurant, chances are about 50/50 you will be carded when ordering from a waiter. If you are with your parents these odds decrease, with your friends these odds increase. However I have been denied in older company and served with my friends.

Related Web Sites (as of 3/28/98)

How To Spot Fake ID and Not Be Fooled
http://www.cs.usask.ca/undergrads/cwu122/macs.html

The Fake ID Page (Template!)
http://www.users.cloud9.net/~insanity/fakeidpage.html

The Official ID Checking Guide (Very good book! Order it today!)
http://www.webbanker.com/pub2.html

Fake Identification Information
http://members.aol.com/cycore/idinfo.htm

A Page of Fake ID Links
http://members.aol.com/cycore/idlinks.htm

Guide to US & Canadian Drivers License Security Techniques! (Invaluable!!)
http://members.aol.com/cycore/license.htm

In closing, here is a helpful excerpt from *"How To Spot Fake ID and not be fooled"*

"Over the past two years selling cigarettes, I have found there are a number of dead-giveaways minors continually do, but never catch on to. (Some of these cannot be avoided anyway!)

"Minors usually will have their ID ready in their hand as they walk in the door. If this happens, be suspicious.

"On a related note, minors will usually produce ID very quickly after you ask for it.

"Minors will usually produce an abundance of minor ID, such as a student card. This minor ID is usually something that doesn't have a picture or a birthday, just a name. Or they will produce one piece of ID hoping you will take it.

"Minors will usually be nervous. Trembling in their hands or shivering is usual."

letters continued from page 39

when launching IRC attacks. We added the info ourselves because we reached a conclusion similar to yours as to the overall goal of the author.

Mitnick

Dear 2600:

You should consider publishing the following web sites, which provide the e-mail addresses of all of the Senators and Representatives, so that your readers can send a message regarding Kevin Mitnick.

http://www.house.gov/writerep/

http://www.senate.gov/senator/membmail.html

Misaline

Dear 2600:

I'm a new subscriber to your fine magazine. I've bought it newsstand for a few years, but decided with the rise of your distributor problems to send the money direct to support the cause. I've also bought some stuff and tried to do my best to help things along financially and psychologically by talking to others about 2600, the hacker community, and the related topics therein so as to set the record straight on some things.

This brings me to my question: after learning more about the Mitnick case, I want to do my part to help the man out. I've already sent some money his grandmother's way (not much, but it's all I can spare). However, I've been considering writing up my own FAQ sheet on what exactly Kevin did, statistics about how long he's been incarcerated, what civil/human rights have been broken, etc. After I compiled this information, I would arrange it in an easy-to-read flyer and start distributing it in electronic and real form wherever I could. If people liked the idea, they could use it freely, or improve on it in their own communities.

As such, I have an unusual request: my web access, when I do manage to scrape it together, is very limited - Lynx at best with limited download capacity. I've seen the Mitnick site but it doesn't have the quick-and-dirty facts that I want easily available. I tend to get lost in the legalese, and being a relative newcomer to the actual facts behind the case (I wasn't following it for a long time, admittedly, only within the last few months has it started to take a hold on me), I haven't been able to put together everything I'd need to build a flyer.

So, if 2600 could publish a quick synopsis of the Mitnick case in the next issue, or if someone there could email me something similar, I would appreciate it. After I have created the flyer, I would naturally snail-mail one to 2600 for the viewing pleasure of those of you there so you could use it.

The only way Kevin Mitnick is going to see freedom at this point is if he finds a groundswell of public support - while merely the hacker community helps, the great unwashed have a very high success rate when it comes to setting public policy. America is still vaguely a democracy - those of you in America ought to remember this. Write your Congressman, circulate petitions, get public awareness up there. No matter what you may think, every American citizen has a little power to change things. Try it - the worst that could happen is that it has no effect. Fight the good fight.

*69

We've already devoted many pages to the Mitnick story since 1995 - the best thing to do is go through those articles and gather facts in that way. We now also operate the official Kevin Mitnick web page at www.kevinmitnick.com which should have everything you're looking for. We hope your inspiration spreads.

Dear 2600:

Tell Howard Stern about him. He doesn't seem to like the government.

ed

Well, if that's the only prerequisite, how about we tell the American public instead?

Head Hacking Advice

Dear 2600:

I enjoyed the article in the Winter Edition (14:4) called "Hack Your Head." I have actually found the *best* way to stay awake and would like to share it with the world thru 2600.

Get a bottle of Jolt and bring it to a boil. Next, add it to 3-4 tablespoons of freeze-dried coffee. The drink itself is pure heaven. This thing has kept me going 10-15 hours *non stop*. Try to drink a glass of OJ straight afterwards. Its vitamin C increases your alertness by about 30 percent.

Malibu

Dear 2600:

I agree that that the combination of stimulants mentioned in your article is the best and safest choice. One thing, you should use them every day and get at least one good night of sleep a week. I know this cuts into our hacking time but being human we have to. Besides, sleeping helps you think better and clear your body of jitters so you can solder again. Also, not getting enough sleep could cause problems in the long term. Keep up the good articles.

Kevin g

Clarification

Dear 2600:

Hey, I hate people who equate hackers with criminals just as much as you do, but I thought this one needed clarification. On page 49 of the Autumn 1997 issue, an AOLer writes in saying his "leader" of the "warez group kryp-" found out how to get free calls using 1-800-COLLECT. He attaches a CC#, and some numbers to dial.

My idea is he got this from another document. But the CC# is supposedly a *dead card*. That's why he said "Punch in 00000 as the zip code." According to this document, you can do the same thing talking to an operator and telling them it's an international card. The zip code then isn't checked against the card. However, the service has stopped being automated.

In regards to Agent Steal's article, I learned a great deal from it. I personally don't care that he went to go work for the FBI (well actually, I do, but I still am quite in favor of the publishing of the article). If all the FBI agents had this much to share with us and felt this way about hackers in general, we wouldn't have half the problems we have today. I don't believe your articles should be screened just by judging the person who wrote them. If there's something illegal about it ("Hack the Vote" springs to mind), that's entirely different, but anyaNIg (who wrote in the Winter 97-98 issue saying it seemed a little traitorous to publish an article by Agent Steal) is somewhat mistaken. The article was very informative, and I don't believe it should be the last we hear from him - if the rest of his articles are up to par.

Afrikz

Dear 2600:

I've reread the Winter 97-98 mag again and I have to clear something up. That guy Morris says he was trained with people who were given the option of enlisting in the Military (USAF) or going to jail. I joined the Air Force when I was 18 as a Security Specialist (SP) and I have *never, never ever* run across anyone who has been given this option. Why, you ask? As a person in one of the most veteran career fields in the Air Force, I have met my share of scrubs and criminals but not one was there because of a "court ordered choice." That is quite a load of crap. Morris noted their crimes were drug violations - *big negative!* USAF doesn't mess around with drugs... I admitted to only being present when people were smoking weed and I had to go see a Head Shrinker every freakin year except one. Knowing the Air Force and these times, they might be willing to work with "electronic intruders" but I haven't seen that either.

K. Ruff

Bookstore Monopolies

Dear 2600:

2600's experience with Barnes & Noble reminds me how dangerous it is to have a couple of big bookstore chains control so much of the market.

You may be interested to know that Barnes and Noble, as well as Borders/Walden, have been sued for antitrust violations by the American Booksellers' Association (ABA) and more than 20 independent bookstores. The ABA says that the large chains are cutting secret, sweetheart deals with publishers that give them an advantage over independent bookstores. Without a level playing field, the independent bookstores are then unable to compete, and end up going out of business. (For more information, visit ABA's web site at www.bookweb.org.)

With the market dominance they have, the big chains can do what Barnes & Noble may have done to 2600. If they decide that a publication is undesirable - for whatever reason - they can effectively block millions of Americans from ever seeing it, just by keeping it off of their own shelves. Worse still, they could use excessive returns to bankrupt a small publisher, and make sure that it never publishes again!

Even the biggest publishers would hesitate to offend the chains they count on for so much of their sales. Freedom of the press could soon mean "freedom to read what Barnes & Noble and Borders/Walden consider acceptable."

For more dirt on the big bookstore chains, check out www.booksellersunion.org on the Web.

R.J. Eleven

Independent bookstores will always be high on our list of places where we want 2600 to be found. Unfortunately, the nature of American business seems to reward monopolizing the marketplace - we see it in telecommunications, software, chip manufacturing, broadcasting, and now even books. The difference in the latter example is that reading material lends itself to being different and critical of the established order of things. People go to bookstores, not out of brand loyalty, but because they're interested in the ideas being presented there. The proliferation of bookstores is a good thing for the most part, even if the major chains wind up in every town. You stand a far better chance of learning something there than in a video arcade. But if the same business practices common in corporate America are allowed to take hold in these chain bookstores, the potential for thought control will be staggering. We can't imagine such things happening without a fight, considering the fact that most people who frequent bookstores have half a brain to begin with.

Credit Due

Dear 2600:

I know you don't have time to go through *all* of your articles that you print and run background checks and whatnot, but this really pissed me off. Vandal, who

claims to have written the article "ANI 2: The Adventure Continues" (Spring 98) is a plagiarist. The moment I read his article I knew it looked familiar. I went to one of the most informative sites on the web, www.nanpa.com, and boom, there's an identical copy of his article. Here's the address; look for yourself: http://www.nanpa.com/number_resource_info/ani_ii_assignments.html. Anyhow, I hope you print this because although that article was extremely informative, Vandal can't take credit for what he didn't write. I'm not blaming this on the editors, simply defaming Vandal and discouraging this type of action in the future.

Nothingg

Here is Vandal's reply:

"Unfortunately, I was a few days late mentioning to 2600 staff that I had included information directly from NANPA.com in my ANI II article. I was completely aware of this copying, and simply want to clarify that most of my article's information/research could be found on NANPA.com. However, I was unaware that, even if acknowledged, the copying was wrong. This was, obviously an honest although absent minded and ignorant mistake, and a mistake I'm sure anyone could make. Words for any prospective writers: Don't copy directly, even if it is acknowledged! You're better off, and completely 'out of trouble' if you paraphrase any research from other sources, such as web sites or other articles.

"On a personal note, please accept my apologies for any confusion having to do with a lot of the information of my article. I tried to attach acknowledgements, but by the time it got to 2600 staff, the issue had already gone to press. So, keep in mind that everything after the third paragraph is not written by me. It comes from NANPA.com and should be used as resource/research. It was meant to simply 'back up' my original article. My article can thus be considered the outline and information regarding the two-digit line-ID. The research information were the line-ID numbers that followed (99-99)."

Phone Exchange History

Dear *2600:*

I loved the look back at the history of telephone exchanges article by Jeff Vorzimmer. This is a subject that doesn't get enough attention. I mean, we are talking about the preliminal origins of our community.

One thing that Jeff Vorzimmer didn't mention is the expansion from the five digit telephone numbers to the new seven digit number. At first when dialing came about in the 1920's the exchange would have two letters and then a three digit number. Only the big cities (such as New York, Boston and Philadelphia) were expanded to seven digits (hence Pennsylvania 6-5000) first but the rest of the country kept five digit numbers much longer. Rural, western sections of the USA had five digit numbers up to the early 1970s!

How do you know if you have an old five digit exchange? The expansion occurred by placing a one at the end of the exchange and a zero before the last three digits. So BA-234 would be BA1-0234 and listed as 221-0234. Most of the old five digit numbers are found in Centrex blocks and given to business customers but there are old residential and government numbers still in use from the five digit days.

Also, an article about the old Western Union telegraph network of the 19th century would be good but that is another piece of text after a bit more research.

Stealth Ricochete

A Suggestion

Dear *2600:*

After reading the very interesting page on the Secret Service and their involvement with the Pentagon Mall and Betsie, I have come to this conclusion. I know that holding public protests help a great deal, but how about instead of having people actually go to the place, why don't people do the following: Call up a major radio station. You might think it would be dumb, but if at least 20 people call in one day and start complaining about incidents, and if someone actually goes on the air live and speaks, it would help a great deal and the word would spread, considering the media hasn't helped. I mean, don't just call up and protest. Request a song, and be like, "By the way," etc. Anything would work. Not everyone has the Internet and some of those people when they hear the word hacker, they shudder. Any radio station would work, and if the word gets around about the Secret Service and these incidents, it would be a great help.

F.E.D.-D.E.F.

You operate under the misconception that commercial radio stations care about the local community. Thanks to the FCC, there really aren't very many local stations left - most are owned by the same mega-corporations and the few alternative voices on the dial have been silenced. Your suggestion is a good one and in a better society would work well. Until things start to change on the radio dial, it just won't work here.

The Generation Gap

Dear *2600:*

I noticed a letter in your Winter 97-98 issue from Spektor where he/she talked about how older generation hackers look at younger hackers as "malicious little bastards." Well I too have seen that happen. I am 14 years old, and I know more about computers and phones than a lot of people I meet, and the people I meet are the ones who think they are "a badass hacker dude." These people are mostly older folks. I get crap all the time about my age and being some "wannabe little kiddie" and I am sick of it. I feel that anyone who looks down on younger people like myself can go shove a stick up their ass. I program in three languages and have a great understanding of UNIX and its many variations. This letter may make me sound retarded, but I think that you in the older generation out there should have some respect for younger folk who know just as much, or more than you. Just remember that next time you go to a 2600 meeting and see a 14-year-old, or talk to a younger kid somewhere - treat him like he is a normal human, and do not exclude him from a conversation. I am shutting up now. Thanks.

curtis la cali

You should also remember there's words both ways - don't judge older people in ways you wouldn't want to be judged yourself. Also, you will one day become one of these older people. Hopefully you will retain your respect of 14-year-olds when that happens.

More on FYROM

Dear *2600:*

I read Chris Paraskeyopoulos's letter in the 15:3 issue and your answer. I have to say that your point of view is not correct. The name Macedonia "belongs" to Greece since 400 years B.C., and no one can claim it for his own little country. I believe that this is a mistake of you and not something that was done on purpose. I do not want to seem impolite, but I had to say this about Macedonia and FYROM, though FYROM is not a very respectful name for a newfounded country.

MB Mastermind
Athens, Greece

Sigh. One comment about this region of the world and we'll never see the end of it. OK, very simply, since you're already calling the country the Former Yugoslav Republic of Macedonia, what's so bad about referring to it as Macedonia to save a little time? You've already acknowledged that this was the name of the republic. Does it have some other name? If so, then let's use that name. Yes, we know that part of your country also calls itself Macedonia and the Greek Macedonian borders the other Macedonia. We've lived in a world with two Germany's, two Korea's, two Congo's, and two Yemen's. We even had two Pakistan's once. So why not call them North Macedonia? Or take your Macedonia and shake and make a Greater Macedonia. We're sure you'll think of something. Anything is better than FYROM.

A Nagging Question

Dear *2600,*

I just recently got the Volume 14 Number 4 edition and I feel that I need to ask you guys something that has been bugging me for a long time. Who the hell are the old men modeling the 2600 t-shirts? I'm not sure if they are the same person, although it doesn't look like it, but I'm very curious to know. Those guys look very cool in those shirts and if I can look half as cool as they do, then I'm buying myself a couple of those shirts. Thank you very much - now I might be able to sleep good at night.

Trend_Killa

The gentleman in our black shirt with the military head and white hair is Lieutenant General Kenneth A. Minihan, who holds the title of DIRNSA (Director, National Security Agency). The man sporting our white shirt is William P. Crowell, the former DEPDIRNSA (Deputy Director, National Security Agency). (The new DIRNSA, incidentally, is Barbara McNamara. We're still trying to find a shirt that will do her justice.) Both of our models' photographs appear on the back side of the black shirt, along with the pretty NSA seal.

Immortalize Yourself

Send your letters to:
2600 Editorial Dept.
P.O. Box 99
Middle Island, New York
11953-0099
or e-mail letters@2600.com

Happenings

DON'T FORGET INFOWARCON 98! September 8-11, 1998 at the Hyatt Regency Crystal City, 2799 Jefferson Davis Highway, Arlington, VA 22202 (call (703) 418-1234 for special rate). Produced by Winn Schwartau and MIS Training Institute. Registration for conference: $895. conference & two tutorials: $1385. Registration Manager, MIS Training Institute, 498 Concord St., Framingham, MA 01702-2357. The complete conference brochure and registration is available at: http://www.misti.com/infowar98/.

For Sale

CONSOLE BACK-UP DEVICES: Looking for console back-up devices for your Nintendo64, NES, SNES, and Gameboy? Wanna play all the games for free? Come to Vivid Barrier at http://surf.to/vividbarrier/. We got good prices and lots of selection.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $20 ppd; Forbidden Subjects CD-ROM (330MB of hacking files) $12 ppd; Disappearing Ink Formulas - safely write memos, love letters, or nasty notes. Fade time is adjustable. $5 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

HACK THE RADIO: Hobby Broadcasting magazine covers DIY broadcasting of all types: AM, FM, shortwave, TV, and the Internet. It includes how-to articles about equipment, station operation and programming, enforcement, and much more. For a sample, send $3 U.S. ($4 Canada or $5 international). A subscription (4 quarterly issues) is $12 in the U.S. Hobby Broadcasting, PO Box 643, Mont Alto, PA 17237.

OFFERING SIX VIRUSES/VIRI which can automatically knock down DOS and Windows 3.1 operating systems at the victim's command to open Windows. Easily loaded, recurrently destructive, and undetectable via all virus detection and cleansing programs with which I am familiar. Well-tested, relatively simple, and designed with stealth and victim behavior in mind. Well written instructions, documentation, and antidote programs are included. $5 even TOTAL! Cash, money orders, and checks accepted. Sorry, no foreign orders. Provided on seven 1.44 MB, 3.5" floppy disks which can be freely copied. They make great gifts! Orders are promptly mailed out "priority" (USPO). Satisfaction guaranteed or you have a bad attitude! The Omega Man, 219 Lexington Rd., Elgin, TX 78621-1645. omegaman4@juno.com.

INFORMATION IS POWER! Get our catalog of informational manuals, programs, files, books, newsletters and videos for only $1 (S&H). Our products cover information on hacking, phreaking, cracking, electronics, virii, anarchy and the Internet. Legit and recognized world-wide. Send your $1 US to: SctMESC, Box 573, Long Beach, MS 39560.

PADLO'S ONLINE: http://www.padlos.com. Entry equipment, automatics, police, covert, and exotic weaponry. By professionals, for the professional. We GUARANTEE your satisfaction, and lowest prices ANYWHERE on ANY MERCHANDISE. Many exclusive items, serving you since 1996, now with on-line ordering!

BROADEN YOUR MIND! I am selling the following information for cheap. Set up Windows 3.xx with multiple configurations. Complete code and instructions to give each user different wallpaper, screen savers, even screen resolutions! Much more! Only $4.00. How to change the startup graphic in all Windows versions. Bonus: how to change Win 95/98 exit screen. All for only $2.00. Pamphlet on how to hide files, e-mail, etc. in a graphic picture. Can store files up to 200k. Requires programming knowledge. Only $2.00. Send cash, check, or money order (preferred, for fastest service) to: John D. Lord, PO Box 488, Boonville, IN 47601.

INFORMATION ARCHIVES: All the stuff you've always wanted to know but were afraid to ask! SOURCE CODE SPECIAL: source codes for the following exploits: ICQ Sniffer, Mozilla Killer, Pentium Killer, the infamous Win95 "Bonk" attack and many more - $10 each. Hard copies of PHRACK, hacker utility disks, and, as always, INFORMATION! For catalog, please send $3 along with one 32 cent stamp to: Information Archive Catalog Request, J. Olsommer, PO Box 222, Lakeville, PA 18438.

ATTN DIRECTV USERS: Learn how to get free pay per view events, movies, specials. Send $6.50 cash or check made out to CASH. Send to TV Ripoff, 11597 Beech Ave. #2600, Palm Beach Gardens, FL 33410-2605.

TOP SECRET CONSUMERTRONICS, exciting hacking, phreaking, and weird products since 1971. Go to www.tsc-global.com or send $3 for catalog to: Box 23097, ABQ, NM 87192.

Help Wanted

OFF THE HOOK can now be heard on the net! Thanks to the generosity of people with access to bandwidth, people from around the planet can tune in every Tuesday at 8 pm Eastern Time by connecting to www.2600.com (listeners in the New York metropolitan area should tune to WBAI 99.5 FM). If you have access to a T-1 or better from work, your dorm room, or anyplace else in the entire world, we need your help to get the show distributed. Mail porkchop@2600.com if you have the bandwidth to serve listeners from around the world.

LUCRATIVE JOINT VENTURE. "Top Gun" hacker or surveillance expert needed. Call in complete confidence: Ross (612) 306-1245.

SEEKING HELP on how to identify unauthorized duplications of computer software programs by corporate entities. Possible reward for those who can help. Please respond to: Martin Drost, 4949 W. Dempster, Skokie, IL 60077.

Wanted

WE WANT TO BUY DATABASES. We will purchase any public or private database that contains name (or company name) / address / telephone number / date of birth / ssn, etc. or any combination of the above - i.e., driver licenses, motor vehicles, voter registrations, criminal records, corporate records, real property, UCCs, etc. Foreign databases also purchased. Immediate cash paid. Send details to: Mr. Data, POB 155, Midwood Station, Brooklyn, NY 11230.

DO YOU NEED NUMBERS? I want interesting toll-free 800/888 phone numbers such as ANI's, CNA's, PBX's, voice systems, computers, weird numbers, or anything else. I will give you TWO numbers from my collection for every ONE number you send me. Please e-mail all numbers to: ender301@juno.com.

Services

CHARGED WITH A COMPUTER CRIME? Contact Barsey Morrow, Jr., Attorney at Law, at (334) 365-6602 or cyberlaw@mindspring.com. Extensive computer and legal background.

Personal

I NEED SOME INTELLECTUAL STIMULATION! Help me! I am trapped in a big federal prison with 1,300 bums and nuts! You can HELP ME ESCAPE boredom and insanity! Quickly gather up computer books and magazines, software manuals, and related materials, a paperback dictionary, thesaurus, book of antonyms and synonyms, etc. Send them to me. A mind is a terrible thing to waste! Tom Proctor, FCI 28204-004, PO Box 1000, Petersburg, VA 23804.

BOYCOTT BRAZIL. Please review my web sites and help me inform the WORLD as to my torture, denial of due process, and forced brain implantation by Brazilian Federal Police in Brasilia, Brazil during my extradition to the U.S. Snail mail appreciated from volunteers. John G. Lambros, #20436-124, USP Leavenworth, PO Box 1000, Leavenworth, KS 66048-1000. Web site: http://members.aol.com/BrazilByt.

ONLY SUBSCRIBERS CAN ADVERTISE IN 2600! Don't even bother trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Autumn issue: 9/15/98.

lies continued from page 5

a mere 20 minutes into the film. Shimomura, in a sobering tone, warns his girlfriend: "He could be... reading your mail. Listening to you, when you talk on the phone. Looking at your medical records. What your shrink said, when he sent in the forms, to the insurance company. What kind of gear you ordered from North Face. Whether you like down, or Thinsulate. Your college transcript. Your credit card statement. How many times you went to the drugstore, and what you charged." It's just like *The Net* except Kevin Mitnick replaces today's society as the primary threat to privacy. As we progress, concern over Mitnick's capabilities grows: "He could be going into medical records, fucking them up. He could be killing people, and we're just standing here." In fact, as Mitnick suspects he is about to be caught, we see him actually trying to change someone's medical records - which is about the dumbest thing anyone in such a situation could ever do. Then the FBI becomes concerned over Mitnick's ability to wriggle out of the situation. "Every step of what we do will be scrutinized. Did we have the warrant for this? Did we have the right to do that? *He* won't be on trial. *We* will." There is no mention made of the fact that the feds have so far managed to lock him up *without trial* for three and a half years. That's something the makers of this film clearly don't think the American public needs to know.

From the opening scene where Mitnick is shown as a foul-mouthed, cheating 12-year-old to the end where he gets his just deserts in prison, we see Mitnick lie, steal, and hack his way across America, stopping long enough to unleash racial epithets towards the film's noble hero Shimomura. ("I think that man needs a haircut. I mean, he can cover his ears, but I, for one... well, I still remember Pearl Harbor." Or "I cannot fucking believe what I hacked out of Japboy.")

Not surprisingly, Markoff's involvement in the search and capture is erased completely. And Shimomura is made into someone with compassion who actually reaches out to Kevin while he's in prison, attempting to make peace and saying he's sorry it had to be like this. In real life, Shimomura has never said a word to him.

Mitnick, who will be played by Skeet Ulrich of *Scream*, is made out to be nothing less than a demon, who doesn't care who he hurts and who will stop at nothing to get what he wants. He equates his life to a video game, if you can believe that: "It's like Pacman. There's food. You find it. You eat it. You stay alive. Then there's a couple of ghosts chasing you. They find you, you die. That's it." By the end of the film, you will be so happy he's behind bars that you will start searching for "Free Kevin" stickers to rip down.

Technical inaccuracies abound, like the typical Hollywood perception that modems are always screeching in the background. Or this stage direction: "He takes a long chug of his Big Gulp, wets his lips, licking them thoroughly. Then picks up the phone, waits for the dialtone, and... whistles. It's not a tune. It's the tones of the touch-tone system, and Mitnick is whistling in his own code."

Most of the characters who are not named Shimomura are seen as bumbling idiots or vindictive assholes who let their personal dislike of our hero get in the way of the investigation. In a real stretch of the truth, the staff of San Francisco's The WELL, refuse to erase Shimomura's sensitive data that Mitnick supposedly uploaded via a hacked account. They say, "it's the policy of The WELL not to change, censor, tamper with, or delete the work of our users. It's not ours. It's theirs." Of course, anyone in their right mind would realize that an *unauthorized* user would never be given the same rights as an authorized one! This is clearly not the way it happened at all.

The only real dramatic tension comes from making Shimomura into someone with a secret past who had files that could destroy the world or something - the details are never gone into. And Mitnick is his evil counterpart who intends to spread these files to the world: "Sooner or later, he's gonna upload. The OKI data, the credit cards... my, ah, Los Alamos files." Yeah, right, whatever.

But easily the most bizarre and offensive part of the film comes when Shimomura and Mitnick come face to face in Seattle, an incident everyone admits is completely fabricated. "Just as Shimomura relaxes... *THWACK!*... he's clubbed on the side of the head. Mitnick, wielding the top of a metal garbage can like a weapon, sees Shimomura drop into the muck. He staggers out of the alleyway. Shimomura, dazed, blood flowing freely from a gash above his ear, raises himself to his elbows... and watches Mitnick disappear, into the night." Mitnick thus graduates from evil, destructive, racist hacker to violent criminal.

There is nothing and nobody to back up any of the absurd allegations in this movie. From the people who know Mitnick to the news reports that did their best to demonize him to the court records that document his repeated failure to be treated fairly, even to the book that this film is based on, there is *no evidence whatsoever* of the kind of despicable criminal behavior portrayed in the script.

So how could such a libelous piece of trash even be attempted? This is the interesting part. Since Mitnick is considered a "public figure," the Hollywood people figure they can get away with bending the truth while using real names. But, as indicated above, the only reason Mitnick is a public figure is because of the antics of John Markoff and Tsutomu Shimomura. Without the two Markoff books and all of those front page articles which wound up feeding hundreds of other newspapers and magazines around the world, how much of a public figure would Mitnick really be? For that matter, would the government have made such a point of keeping him locked away for so long? These are most troubling questions.

But even more troubling is the prospect of such a film being made without the opportunity to set the record straight. Think of what it will mean. For the millions of people who pay to see it, *this* will be the story of Kevin Mitnick. Whenever his name comes up in conversation or in the news, the image from *Takedown* is what people will remember. For that reason alone, action must be taken to stop this.

We have absolutely no problem with bad films being made. And if this were a work of fiction, we'd either trash it when it came out or ignore it completely. But *Takedown* is purported to be documenting a true story and its distortion of the truth will gravely hurt some very real people. How likely is it that Mitnick will be able to get a fair trial (if he's ever allowed to have one at all) once people have seen this film? Oddly enough, his trial has already occurred at the end of the film which only further confuses the issue. Incidentally, legal experts tell us that the two charges he's convicted of in the film (probation violation and "Felony theft of intellectual and real property in violation of Section 6 of the Penal Code" would never get him a sentence approaching the amount of time he's already been in prison. But why confuse the public with facts?

We find this outrageous. And so do a whole lot of other people who have been getting involved in the "Free Kevin" campaign. The movement was already picking up steam when this news hit. Now it's growing faster than we anticipated.

We intend to stop this production in its tracks and make damn sure everyone involved is aware of the facts. And if we are unable to change this reality-based story into something resembling reality, then we will use it as a vehicle to get our own message out. This will include pickets, boycotts, phone/letter/fax campaigns, whatever it takes. There is a story here - a really good one. And while we may not be able to get someone to tell that story, we *can* do something about the lies. We will either stop them or we will make the world aware of what they really are.

If you want to help out, you can contact us at any of the numbers or addresses on page 3 or listen to our weekly radio show Tuesday nights at 8 pm ET (99.5 FM in New York and www.2600.com/radiohack on the net).

Here are the addresses and numbers for the two main Miramax offices. Please make your feelings known!

7966 Beverly Blvd.
Los Angeles, CA 90048
(213) 951-4200
(213) 951-4315 fax
and
375 Greenwich St., 3rd floor
New York, NY 10013
(212) 941-3800
(212) 941-3949 fax

We also encourage you to continue showing support by spreading the "Free Kevin" stickers around as much as you can. Remember, the money we raise through the stickers goes straight to Mitnick's defense fund. The more of these we can get in public view, the more people will become aware of the other side of this story. Make your checks/money orders out to Kevin's grandmother, Reba Vartanian, and mail them to us - 2600 Bumper Stickers, PO Box 752, Middle Island, NY 11953. The stickers are $1 each, minimum order is $10.

As always, we thank you for your support. This is going to be one interesting summer.

More on DSN

by DrSeuss of the OCPP

Overview of the DSN

Unbeknownst to most phreaks, the AUTOVON proper was taken off-line decades ago. In this day and age a new system has arisen that enhances the former AUTOVON and all other military voice/data systems: the Defense Switched Network. The DSN was the result of a swift kick in the ass to the aging military phone network, replacing analog switches first with 5ESS systems and then with a variety of smaller switches.

The DSN was built by AT&T and originally based on 5ESS switches located all over the world. The DSN is divided into two parts. The everyday transmissions are run over the so-called "Black DSN" while secure information is transmitted over the secured "Red DSN."

Black DSN

The Black DSN is an unsecured automatic phone system serving the US military and related government agencies around the world. The Black DSN consists of an unspecified number of Siemens (EWS-4100) and Nortel (SL-100) switches maintained by GTE employees. All Black switches are polled by the Regional Central Center for faults on a regular basis by a system called A100MSS, and all outages and other problems are sent from there directly to the Chief of Operations.

While the DSN itself is considered insecure, the use of STU III voice encryption telephones is standard procedure.

Like the AUTOVON before, a central feature of the Black DSN is the multi-level precedence preemption (MLPP), a slick military term for priority routing.

As mentioned in the Spring issue, Black DSN numbering is handled on an NPA-NXX-XXXX format. The 312 NPA serves CONUS (CONtinental United States) and Canada, the 313 NPA serves the Caribbean, the 314 NPA serves Europe, the 315 and 317 NPAs serve the Pacific and Alaska, and the 318 NPA serves Southwest Asia.

The Black DSN has a BBS that can be reached by telnetting to: dsnbbs.ncr.disa.mil or calling 703-735-8178.

The Black DSN phone directory can be found at:
http://dsnbbs.ncr.disa.mil/phone97/dsn1097.txt

Red DSN

Red DSN is a secure automatic phone system serving the US military and related government agencies such as the National Command Authority (NCA), the National Military Command Center (NMCC), the Airborne Command Post, the Commanders-in-Chief, select military departments, and "Allies of the United States" around the world. Unlike the Black DSN which fulfills the role of a mundane telephone system, the Red DSN is a high security communications system designed for classified and other highly sensitive data.

GTE designed and built the DRSN and still holds most of the contracts for maintenance and security analysis of the Red network. They're also happy to give out colorful diagrams and paperwork to anyone who asks. Raytheon E Systems is the main switch vendor.

Hardware

The Defense Red Switched Network currently consists of a core of Raytheon Secure Digital Switches interconnected and maintained by government personnel (specifically the DRSN Ops Branch) and GTE employees. Medium Digital Switches and Digital Small Switches are used as peripheral switches for small or temporary installations where installing a DEC Alpha would be difficult or impossible.

STU IIIs are the standard Red telephone set. These sets are connected to the switch by physically secured, unencrypted local loops forming so-called red enclaves. Encrypted T-1 trunks interconnect Red switches between enclaves.

Control

(The following information is sketchy. Resources on the DRSN are contradictory about its control.) The DRSN control hierarchy is three tiered. Groups of switches are directly controlled on a local level by a set of Regional Control Centers (RCCs) scattered around the theater. The RCCs are in turn provisioned by the Red DIMSS, which is in turn monitored by the Manager Of Managers system for faults. All alarms are catalogued in a central database at this level.

The DRSN maintains multi-level precedence preemption (MLPP), a slick military term for priority routing of calls, with an additional feature called Ruthless Preemption (flash override-override). This is a level of call precedence that will route over all other calls. Access to this feature is understandably tightly restricted.

Numbering

DRSN switches have a unique numbering scheme involving four types of numbers.

Hotlines. These are five-digit numbers that are generated within a switch that will allow calls to be set up in a point-to-point manner. Hotlines are numbered from 10,000 to 17,999.

Pseudos. These are five-digit numbers that are used internally within a switch for the processing of preset conferences. These numbers are assigned to boards created by software only. 18,743 to 18,999 are used for pseudos.

Trunks. These are five-digit numbers that are used to interface a switch to the DRSN. Numbers 19,000 to 19,999 are reserved for trunks.

Subscriber Directory Numbers (SDNs). These are four-digit suffixes (npa-nxx-XXXX) that are assigned to the individual users.

DISA is in the process of testing new switches for the DRSN. The integrated command switch, small portable switch, medium digital switch, and digital small switch. All switches are designed to interface seamlessly with the existing DSN, DRSN, Highband satellite, and current tactical phone networks.

The DRSN BBS can be reached by telnetting to dnsbbs.ncr.disa.mil. This BBS serves as the main distribution site for the DRSN directory. This isn't a public BBS and getting an account is a tight process. Actual BBS security is unknown.

M E E T I N G S

UNITED STATES

Alabama

Birmingham: Hoover Galleria Food Court by the payphones next to Hardee's. 7 pm.

Arizona

Phoenix: Peter Piper Pizza at Metro Center.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Sacramento: Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9544 - bypass the carrier.

San Diego: Burnsshell on Regents Road (Vons Shopping Mall).

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Connecticut

Milford: The Post Mall by Time Out.

District of Columbia

Washington: Pentagon City Mall in the food court.

Florida

Ft. Lauderdale: Pompano Square Mall (SW corner of US 1 and Copans Rd.) in the food court.

Ft. Myers: At the cafe on Daniels and Mable.

Miami: Dadeland Mall on the raised seating section in the food court.

Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648, 896-9708, 895-9844, 8265.

Pensacola: Cordova Mall, food court, tables near KFC. 5:30 pm.

Georgia

Atlanta: Lenox Mall Food Court.

Illinois

Chicago: Pick Me Up Cafe at 3408 North Clark Street.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8822 - good luck getting around the carrier.

Maine

Portland: Maine Mall by the bench at the food court door.

Massachusetts

Boston: Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Northampton: Javaline Cafe at 241 Main Street.

Michigan

Ann Arbor: Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Missouri

Kansas City: Food Court at the Oak Park Mall in Overland Park, Kansas.

St. Louis: Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Nebraska

Omaha: Oak View Mall, Barnes and Noble, 6:30 pm.

Nevada

Reno: Meadow Wood Mall, Palms Food Court by Sbarro, 3-9 pm.

New Hampshire

Nashua: Pheasant Lane Mall, near the big clock in the food court.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain and arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

New York

Buffalo: Eastern Hills Mall (Clarence) by lockers near food court.

New York: Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Rochester: Marketplace Mall food court. 8 pm.

North Carolina

Charlotte: South Park Mall, raised area of the food court.

Raleigh: Crabtree Valley Mall, food court.

Ohio

Akron: Arabica Cafe on W. Main St.

Cleveland: Coventry Arabica. Cleveland Heights, back room smoking section.

Columbus: Convention Center, first level near the payphones with red seats.

Oklahoma

Oklahoma City: Shepard Mall, at the benches next to Subway and across from the payphones. Payphone numbers: (405) 942-9032, 9288, 9391, 9404.

Oregon

Portland: Pioneer Place Mall (not Pioneer Square!), food court.

Pennsylvania

Philadelphia: 30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westtown Mall.

Memphis: Wellchase Cafeteria.

Nashville: Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

Texas

Austin: Dobie Mall food court.

Ft. Worth: North East Mall food court, Loop 820 @ Bedford-Euless Rd. 6 pm.

Houston: Food court under the stairs in Galleria 2, next to McDonalds.

San Antonio: North Star Mall food court.

Washington

Seattle: Washington State Convention Center, first floor.

Spokane: Spokane Valley Mall food court.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

Milwaukee: Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell and Pulteney Streets.

Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: At the Groenplaats at the payphones closest to the cathedral.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

Rio de Janeiro: Rio Sul Shopping Center, Fun Club Night Club.

CANADA

Alberta

Edmonton: Sidetrack Cafe, 10333 112 Street. 6 pm.

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

Ontario

Ottawa: Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Toronto: Cyberland Internet Cafe, 257 Yonge St. 7 pm.

ENGLAND

Bristol: By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 6:45 pm.

Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds: Leeds City train station outside John Menzies. 6 pm.

London: Trocadero Shopping Center (near Piccadilly Circus) next to VR machines. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

FRANCE

Paris: Place d'Italie IRC, in front of the Grand Ecran Cinema. 6-7 pm.

GERMANY

Munich: Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Brigdspace of Hacker Phone numbers. Payphones: 49 89 591-835, +49-89-558541, 542, 543, 544, 545.

INDIA

New Delhi: Priya Cinema Complex, near the Allen Solly Showroom.

IRELAND

Dublin: Phone boxes opposite Stephen's Green Shopping Centre.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

MEXICO

Mexico City: Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

POLAND

Stargard Szczecinski: Art Caffe.

RUSSIA

Moscow: Burger Queen cafe near TA/TASS (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nikitskije Vorota.

SCOTLAND

Aberdeen: Outside Marks & Spencers, next to the Grampian Transport Hub.

SOUTH AFRICA

Cape Town: At the "Brownstone Cellar".

SPAIN

Granada: Cibercafe Granada in Pza. Einstein near the Campus de Fuentenueva.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

Special Offers

2600 Shirts

The new 2600 shirts have arrived! And the NSA loves them!

Version 1 (see photo below) has a nifty hacker dateline on the back and the latest headlines from the hacker world on the front. Black lettering on white.
$15, 2 for $26

Version 2 (see photo below right) is only for those of you into cryptology. Others are prohibited from owning this shirt. Do not wear this around children or senators. White lettering on black.
$15, 2 for $26

All shirts are printed on high quality 100% cotton. Available in L, XL, and XXL (XL fits most nearly everyone.) $15 each or two for $26.

We also have navy blue Beyond Hope shirts left over from the conference! You can now lie to your friends and say you were there even if you weren't! $12 each or pay $30 total when ordered with any two other shirts - that's ten bucks a shirt! Limited availability - XL and XXL only.

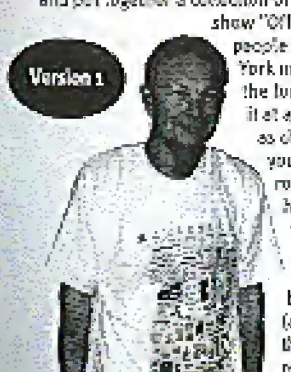
Caps

Stand out in the crowd of people wearing caps. Yes, 2600 caps, suitable for raving, are finally out. Despite the wide disparity of heads, we're assured that this one can be adjusted to fit. Those of you who went on a different evolutionary route may have problems. $10

Off The Hook CD ROMS

After many years, we've finally gotten off our asses and put together a collection of the hacker radio show "Off The Hook" so that people outside the New York metro area can join the fun! And we're doing it at a price that is almost as cheap as turning on your radio. Each cd-rom holds nearly 100 hours of audio. All you need is a computer with a cd-rom drive and browser software (available for free on the net) and a realaudio player (also available for free from www.realaudio.com). You do NOT need net access to play these files! And you can still download our shows one by one off our web site for free!

10/88-12/91 $20
01/92-12/93 $20
01/94-09/95 $20
10/95-06/97 $20



Hope Videos

Another project we took our time doing. From the first HOPE conference back in 1994, the following is available:

The HOPE intro & Robert Steele's speech. 60 minutes ($15)
A guide to Metrocard from a mystery transit worker. 60 minutes ($15)
The LINUX people discuss their OS and Bernie S. talks about TDD's. 100 minutes ($20)
TAP Magazine with Cheshire Catalyst/Dave Banisar on Digital Telephony and the Clipper chip. 105 minutes ($20)
The 2600 panel featuring Emmanuel Goldstein, David Ruderman, Scott Skinner, and Ben Sherman. 60 minutes ($15)
Encryption and beyond with Bob Stratton, Eric Hughes, Matt Blaze, and Bernie S. 120 minutes ($20)
The National ID Card with Judi Clark, Bob Stratton, and Dave Banisar / the famous Social Engineering panel. 100 minutes ($20)
Hacker authors featuring Julian Dibell, Paul Tough, Winn Schwartau, Rafael Moreau, and some of the production staff for "Hackers." 75 minutes ($15)
Cellular Phones with Jason Hillyard, Bernie S., and Mark. 120 minutes ($20)
European Hackers featuring the Chaos Computer Club. 65 minutes ($15)
The Art of Boxing with Billsf and Kevin Crow - Phiber Optik phones in from prison. 105 minutes ($20)
Closing cermonies. 40 minutes ($15)
Order the complete set for only $150!

To Order

Send a list of what you want (be specific!), your address, and your money to:

2600
PO Box 752
Middle Island,
NY 11953